Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 12 (2006) 155–185

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Improved explicit estimates on the number of solutions of equations over a finite field☆

Antonio Cafure[a, b], Guillermo Matera[b, c, *]

[a] *Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I (1428), Buenos Aires, Argentina*

[b] *Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (1613), Los Polvorines, Buenos Aires, Argentina*

[c] *Consejo Nacional de Investigaciones Científicas y Tecnológicas (CONICET), Argentina*

Received 12 May 2004; revised 18 February 2005

Communicated by Gary L. Mullen

Available online 3 May 2005

Abstract

We show explicit estimates on the number of q-ratinoal points of an $\mathbb{F}_q$-definable affine absolutely irreducible variety of $\overline{\mathbb{F}}_q^n$. Our estimates for a hypersurface significantly improve previous estimates of W. Schmidt and M.-D. Huang and Y.-C. Wong, while in the case of a variety our estimates improve those of S. Ghorpade and G. Lachaud in several important cases. Our proofs rely on elementary methods of effective elimination theory and suitable effective versions of the first Bertini theorem.

Keywords: Varieties over finite fields; q-rational points; Effective elimination theory; Effective first Bertini theorem

☆ Research was partially supported by the following Argentinian and German grants: UBACyT X112, PIP CONICET 2461, BMBF–SETCIP AL/PA/01–EIII/02, UNGS 30/3005. Some of the results presented here were first announced at the *Workshop Argentino de Informática Teórica*, WAIT'02, held in September 2002 (see [CM02]).

* Corresponding author. Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (1613), Los Polvorines, Buenos Aires, Argentina

E-mail addresses: acafure@dm.uba.ar (A. Cafure), gmatera@ungs.edu.ar (G. Matera)

URL: http://www.medicis.polytechnique.fr/∼matera (G. Matera).

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.03.003

1. Introduction

Let p be a prime number, let $q := p^k$, let $\mathbb{F}_q$ denote the finite field of q elements and let $\overline{\mathbb{F}}_q$ denote the algebraic closure of the field $\mathbb{F}_q$. Let be given a finite set of polynomials $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ and let V denote the affine subvariety of $\overline{\mathbb{F}}_q^n$ defined by $F_1, \ldots, F_m$. Counting or estimating the number of q-rational points $x \in \mathbb{F}_q^n$ of V is an important subject of mathematics and computer science, with many applications.

In a fundamental work [Wei48], Weil showed that for any $\mathbb{F}_q$-definable absolutely irreducible plane curve $\mathcal{C}$ of degree δ and genus g, the following estimate holds:

$$|\#(\mathcal{C} \cap \mathbb{F}_q^2) - q| \leqslant 2gq^{1/2} + \delta + 1.$$

Taking into account the well-known inequality $2g \leqslant (\delta-1)(\delta-2)$, we have the estimate

$$|\#(\mathcal{C} \cap \mathbb{F}_q^2) - q| \leqslant (\delta - 1)(\delta - 2)q^{1/2} + \delta + 1, \tag{1}$$

which is optimal in the general case. The proof of this result was based on sophisticated techniques of algebraic geometry.

Weil's estimate (1) was generalized to higher dimensional varieties by Lang and Weil [LW54]. Their result may be rephrased as follows: for any $\mathbb{F}_q$-definable absolutely irreducible subvariety V of $\overline{\mathbb{F}}_q^n$ of dimension $r > 0$ and degree δ, we have the estimate

$$|\#(V \cap \mathbb{F}_q^n) - q^r| \leqslant (\delta - 1)(\delta - 2)q^{r-1/2} + Cq^{r-1}, \tag{2}$$

where C is a universal constant, depending only on n, r and δ, which was not explicitly estimated.

Ghorpade and Lachaud [GL02a,GL02b] found an explicit estimate on the constant C of (2). More precisely, in [GL02a, Remark 11.3] (see also [GL02b, Theorem 4.1]) the following estimate is shown

$$|\#(V \cap \mathbb{F}_q^n) - q^r| \leqslant (\delta - 1)(\delta - 2)q^{r-1/2} + 6 \cdot 2^s(sd + 3)^{n+1}q^{r-1}, \tag{3}$$

where s is the number of equations defining the variety V and d is an upper bound of the degrees of these equations. Observe that in the case of a hypersurface H, estimate (3) gives

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta - 1)(\delta - 2)q^{n-3/2} + 12(\delta + 3)^{n+1}q^{n-2}. \tag{4}$$

The proof of this result is based on a sophisticated method relying on a generalization of the Weak Lefschetz Theorem to singular varieties and estimates of the Betti numbers of suitable spaces of étale ℓ-adic cohomology.

On the other hand, the first general estimate obtained by elementary means was given by Schmidt [Sch73] (see also [Sch76,Bom74,LN83]). Generalizing a method of Stepanov [Ste71], Schmidt obtained the estimate

$$|\#(\mathcal{C} \cap \mathbb{F}_q^2) - q| \leqslant \sqrt{2}\delta^{5/2} q^{1/2},$$

where $\mathcal{C} \subset \overline{\mathbb{F}}_q^2$ is an absolutely irreducible $\mathbb{F}_q$-definable plane curve of degree δ and the *regularity condition* $q > 250\delta^5$ holds.

Later on, using an adaptation of Stepanov's method to the hypersurface case Schmidt [Sch74] showed the following nontrivial lower bound for any absolutely irreducible $\mathbb{F}_q$-definable hypersurface H of degree δ

$$\#(H \cap \mathbb{F}_q^n) > q^{n-1} - (\delta-1)(\delta-2)q^{n-3/2} - (5\delta^2 + \delta + 1)q^{n-2}, \tag{5}$$

provided that the regularity condition $q > cn^3\delta^5 \log^3 \delta$ holds for a certain universal constant $c > 0$. Let us remark that, up to now, this was the best explicit lower bound known for an arbitrary absolutely irreducible $\mathbb{F}_q$-hypersurface. He also obtained the following explicit estimate [Sch76]:

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + 6\delta^2\theta^{2^\theta} q^{n-2}$$

with $\theta := (\delta+1)\delta/2$.

Finally, combining (5) with Schmidt's [Sch76] method and Kaltofen's effective version of the first Bertini theorem [Kal95], Huang and Wong [HW98] obtained

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + (\delta^2 + 2\delta^5)q^{n-2} + 2\delta^7 q^{n-5/2}, \tag{6}$$

provided that the regularity condition $q > cn^3\delta^5 \log^3 \delta$ holds.

From the point of view of practical applications it is important to improve as much as possible the regularity condition underlying (5) and (6). Furthermore, estimate (6) may grow large in concrete cases due to the powers of δ arising in the right-hand side of (6). This is also the case of (3) and (4), whose right-hand sides include terms which depend exponentially on n and the number s of equations.

In this article, combining techniques of Schmidt [Sch74,Sch76] and Kaltofen [Kal95] we obtain improved explicit estimates on the number of q-rational points of an $\mathbb{F}_q$-definable affine absolutely irreducible variety V of $\overline{\mathbb{F}}_q^n$. Our estimates in the case of a hypersurface significantly improve the regularity of (5) and extend it, providing a corresponding upper bound. Further, we improve both the regularity and the right-hand side of (6) and exponentially improve (4). Finally, in the case of an absolutely

irreducible variety, the worst case of our estimates improve (3) in several important cases, such as those of low codimension (for example $2r \geqslant n-1$) and those of low degree (for example $d \leqslant 2(n-r)$).

Our methods rely on elementary arguments of effective elimination theory (see Sections 2 and 6). In particular, we obtain upper bounds on the number of q-rational points of certain $\mathbb{F}_q$-definable affine varieties which improve [Sch74,Sch76,CR96] (see Section 2).

Our estimate for a hypersurface is obtained by a combination of ideas of Schmidt [Sch74] with an effective version of the first Bertini theorem due to Kaltofen [Kal95]. Kaltofen's result is based on the analysis of an algorithm that decides whether a given bivariate polynomial with coefficients in a field is absolutely irreducible. In Section 3, we adapt Kaltofen's algorithm in order to determine the existence of irreducible factors of a given degree of the restriction of a multivariate absolutely irreducible polynomial to a plane. This allows us to obtain suitable upper bounds on the genericity condition underlying the choice of a restriction having no irreducible factors of a given degree (Theorem 3.3). In Section 4, we combine this result with a combinatorial approach inspired in [Sch74] in order to estimate the number of restrictions of a given absolutely irreducible polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ to affine planes having a fixed number of absolutely irreducible factors over $\mathbb{F}_q$.

In Section 5, applying the estimates of the preceding section and adapting the methods of Schmidt [Sch76], we obtain the following estimate for an absolutely irreducible $\mathbb{F}_q$-hypersurface $H \subset \overline{\mathbb{F}}_q^n$ of degree δ (see Theorem 5.2), which holds without any regularity condition

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{\frac{13}{3}} q^{n-2}.$$

Furthermore, using the lower bound underlying the previous estimate we obtain the following estimate (see Theorem 5.3): for $q > 15\delta^{\frac{13}{3}}$ we have

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + (5\delta^2+\delta+1)q^{n-2}.$$

Finally, in Section 6 we combine these estimates with elementary methods of effective elimination theory (see Propositions 6.1 and 6.3) in order to obtain estimates for an affine $\mathbb{F}_q$-definable variety (see Theorems 5.7, 7.1 and 7.5). As an illustration of these results, we have the following estimate for an $\mathbb{F}_q$-definable absolutely irreducible variety $V \subset \overline{\mathbb{F}}_q^n$ of dimension $r > 0$ and degree δ: for $q > 2(r+1)\delta^2$, there holds

$$|\#(V \cap \mathbb{F}_q^n) - q^r| \leqslant (\delta-1)(\delta-2)q^{r-1/2} + 5\delta^{\frac{13}{3}} q^{r-1}.$$

2. Notions and notations

We use standard notions and notations of commutative algebra and algebraic geometry as can be found in e.g. [Kun85,Sha84,Mat80].

For a given $m \in \mathbb{N}$, we denote by $\mathbb{A}^m = \mathbb{A}^m(\overline{\mathbb{F}}_q)$ the m-dimensional affine space $\overline{\mathbb{F}}_q^m$ endowed with the Zariski topology.

Let $X_1, \ldots, X_n$ be indeterminates over $\mathbb{F}_q$ and let $\mathbb{F}_q[X_1, \ldots, X_n]$ be the ring of n-variate polynomials in the indeterminates $X_1, \ldots, X_n$ and coefficients in $\mathbb{F}_q$. Let V be an $\mathbb{F}_q$-definable affine subvariety V of $\mathbb{A}^n$ (an $\mathbb{F}_q$-variety for short). We shall denote by $I(V) \subset \mathbb{F}_q[X_1, \ldots, X_n]$ its defining ideal and by $\mathbb{F}_q[V]$ its coordinate ring, namely, the quotient ring $\mathbb{F}_q[V] := \mathbb{F}_q[X_1, \ldots, X_n]/I(V)$.

If V is irreducible as an $\mathbb{F}_q$-variety ($\mathbb{F}_q$-irreducible for short), we define its *dimension* $\dim(V)$ as the transcendence degree of the quotient field $\mathbb{F}_q(V)$ of $\mathbb{F}_q[V]$ over $\mathbb{F}_q$, and its *degree* $\deg(V)$ as the maximum number of points lying in the intersection of V with an affine linear subspace L of $\mathbb{A}^n$ of codimension $\dim(V)$ for which $\#(V \cap L) < \infty$ holds. More generally, if $V = C_1 \cup \cdots \cup C_h$ is the decomposition of V into irreducible $\mathbb{F}_q$-components, we define the dimension and the degree of V as $\dim(V) := \max_{1 \leqslant i \leqslant h} \dim(C_i)$ and $\deg(V) := \sum_{i=1}^{h} \deg(C_i)$ (cf. [Hei83]). In the sequel we shall make use of the following *Bézout inequality* (see [Hei83,Ful84]): if V and W are $\mathbb{F}_q$-subvarieties of $\mathbb{A}^n$, then

$$\deg(V \cap W) \leqslant \deg V \deg W. \tag{7}$$

An $\mathbb{F}_q$-variety $V \subset \mathbb{A}^n$ is *absolutely irreducible* if it is irreducible as $\overline{\mathbb{F}}_q$-variety.

2.1. Some elementary upper bounds

In this section we exhibit upper bounds on the number of q-rational points of certain $\mathbb{F}_q$-varieties using elementary arguments of effective elimination theory and the Bézout inequality (7). The purpose of this section is to illustrate how these arguments significantly simplify the previous combinatorial proofs (cf. [LN83,Sch74,Sch76]), yielding also better estimates than the usual ones in some cases. We start with the following well-known result:

Lemma 2.1. *Let $V \subset \mathbb{A}^n$ be an $\mathbb{F}_q$-variety of dimension $r \geqslant 0$ and degree δ. Then the inequality $\#(V \cap \mathbb{F}_q^n) \leqslant \delta q^r$ holds.*

Proof. For $1 \leqslant i \leqslant n$, let $W_i \subset \mathbb{A}^n$ be the $\mathbb{F}_q$-hypersurface defined by $X_i^q - X_i$. Then we have $V \cap \mathbb{F}_q^n = V \cap W_1 \cap \cdots \cap W_n$. Therefore, applying [HS82, Proposition 2.3] we obtain the inequality $\#(V \cap W_1 \cap \cdots \cap W_n) = \deg(V \cap W_1 \cap \cdots \cap W_n) \leqslant \delta q^r$, which finishes the proof. □

We observe that when $r = n - 1$, i.e. when V is a hypersurface defined by a polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree δ, the lemma implies that the number of q-rational zeros of f is at most δq^{n-1}.

Lemma 2.2. *Let $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$ $(s \geqslant 2)$ be nonzero polynomials of degree at most $\delta > 0$ without a common factor in $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$, and let $V \subset \mathbb{A}^n$ be the $\mathbb{F}_q$-variety defined by $f_1, \ldots, f_s$. Then $\#(V \cap \mathbb{F}_q^n) \leqslant \delta^2 q^{n-2}$.*

Proof. Since f_1, f_2 have no common factors in $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$, we have that $V(f_1, f_2)$ is an $\mathbb{F}_q$-variety of dimension $n-2$. From the Bézout inequality (7) we conclude that $\deg V(f_1, f_2) \leqslant \delta^2$ holds. Then Lemma 2.1 shows that $\#\big(V(f_1, f_2) \cap \mathbb{F}_q^n\big) \leqslant \delta^2 q^{n-2}$ holds. This implies $\#(V \cap \mathbb{F}_q^n) \leqslant \delta^2 q^{n-2}$. □

Let us remark that the upper bound of Lemma 2.2 improves the upper bounds $2n\delta^3 q^{n-2}$ of Schmidt [Sch74, Lemma 4] and $\delta^3 q^{n-2}$ of Schmidt [Sch76, Lemma IV.3D].

Lemma 2.3. *Let $V \subset \mathbb{A}^n$ be an $\mathbb{F}_q$-irreducible variety of dimension $r \geqslant 0$ and degree δ which is not absolutely irreducible. Then the inequality $\#(V \cap \mathbb{F}_q^n) \leqslant \delta^2 q^{r-1}/4$ holds.*

Proof. Let $V = V_1 \cup \cdots \cup V_s$ be the decomposition of V into $\overline{\mathbb{F}}_q$-irreducible components and let δ_i denote the degree of V_i for $i = 1, \ldots, s$. Our hypotheses imply $s \geqslant 2$. Since every q-rational point of V belongs to V_i for $1 \leqslant i \leqslant s$, we see that $V \cap \mathbb{F}_q^n \subset V_1 \cap V_2 \cap \mathbb{F}_q^n$ holds. Therefore, applying Lemma 2.1 we have $\#(V_1 \cap V_2 \cap \mathbb{F}_q^n) \leqslant \delta_1 \delta_2 q^{r-1} \leqslant \delta^2 q^{r-1}/4$. □

If V is an $\mathbb{F}_q$-hypersurface irreducible but not absolutely irreducible, our estimate gives $\#(V \cap \mathbb{F}_q^n) \leqslant \delta^2 q^{n-2}/4$, which improves the upper bound $\delta q^{n-1} - (\delta - 1)q^{n-2}$ of Cherdieu and Rolland [CR96, Theorem 3.1], obtained assuming that $1 < \delta < q - 1$ holds. Indeed, our upper bound is valid without any restriction on q, and for $\delta \leqslant q$ we have $\delta^2 q^{n-2}/4 < \delta q^{n-1} - (\delta - 1)q^{n-2}$.

3. On the effective first Bertini theorem

Let be given an absolutely irreducible polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree δ and let $H \subset \mathbb{A}^n$ be the affine $\mathbb{F}_q$-hypersurface defined by f. Our estimates on the number of q-rational points of H rely on an analysis of the varieties obtained by intersecting H with an affine linear $\mathbb{F}_q$-variety of dimension 2 ($\mathbb{F}_q$-plane for short). For this purpose, we need an estimate on the number of $\mathbb{F}_q$-planes L for which $H \cap L$ has an absolutely irreducible $\mathbb{F}_q$-component of degree at most D, for a given $1 \leqslant D \leqslant \delta - 1$.

Following [Kal95], we analyze the genericity condition underlying the nonexistence of irreducible components of $H \cap L$ of degree at most D. In order to do this, in the next section we introduce an algorithm which, given a bivariate polynomial $f \in K[X, Y]$, finds the irreducible factors of f over K of degree at most D. Then, in Section 3.2 we obtain a suitable upper bound on the genericity condition we are considering.

3.1. An algorithm computing the irreducible factors of degree at most D of a bivariate polynomial over a field K

The algorithm we exhibit in this section is a variant of the corresponding algorithm of Kaltofen [Kal95].

Algorithm. *Factorization over the Coefficient Field of degree at most D*:

Input: A polynomial $f \in K[X, Y]$ monic in X of degree at most δ, where K is an arbitrary field, such that the resultant $\mathrm{Res}_X(f(X,0), \partial f(X,0)/\partial X) \neq 0$, and an integer D with $1 \leqslant D \leqslant \delta - 1$.

Output: Either the algorithm returns the list of irreducible factors of f defined over K of degree at most D, or f will not have irreducible factors in $K[X, Y]$ of degree at most D.

Set the maximum order of approximation needed: $\ell_{\max} \leftarrow 2D\delta$.

For all roots $\zeta_i \in \overline{K}$ *of* $f(X,0) \in K[X]$ *Do steps* N *and* L.

Step N: Let $K_i := K(\zeta_i)$. *Set the initial points for the Newton iteration*

$$\alpha_{i,0} \leftarrow \zeta_i \in K_i, \quad \beta_{i,0} \leftarrow (\partial f/\partial X)(\alpha_{i,0}, 0)^{-1} \in K_i.$$

(Now we perform Newton iteration)

For $j \leftarrow 0, \ldots, \lfloor \log_2(\ell_{\max}) \rfloor$ *Do*

$$\begin{aligned} \alpha_{i,j+1} &\leftarrow (\alpha_{i,j} - \beta_{i,j} f(\alpha_{i,j}, Y)) (\mathrm{mod}\, Y^{2^{j+1}}) \\ \beta_{i,j+1} &\leftarrow \left(2\beta_{i,j} - (\partial f/\partial X)(\alpha_{i,j+1}, Y)\beta_{i,j}^2\right) (\mathrm{mod}\, Y^{2^{j+1}}). \end{aligned}$$

(Observe that $\alpha_{i,j+1}, \beta_{i,j+1}$ are polynomials of $K_i[Y]$ satisfying $f(\alpha_{i,j+1}, Y) \equiv 0 \,(\mathrm{mod}\, Y^{2^{j+1}})$, $\beta_{i,j+1} \cdot (\partial f/\partial x)(\alpha_{i,j+1}, Y) \equiv 1 \,(\mathrm{mod}\, Y^{2^{j+1}})$.)

Set the approximate root:

$$\alpha_i \leftarrow \alpha_{i,\lfloor \log_2(\ell_{\max}) \rfloor + 1} \,(\mathrm{mod}\, Y^{\ell_{\max}+1}) \in K_i[Y].$$

(Next, we compute the powers of α_i.)

For $\mu \leftarrow 0, \ldots, \delta - 1$ *Do*

$$\sum_{k=0}^{\ell_{\max}} a_{i,k}^{(\mu)} Y^k \leftarrow \alpha_i^{\mu} \,(\mathrm{mod}\, Y^{\ell_{\max}+1}) \quad \text{with } a_{i,k}^{(\mu)} \in K_i.$$

Step L: We find the lowest degree polynomial in $K[X, Y]$ whose root is α_i.

For $m \leftarrow 1, \ldots, D$ *Do*

We fix the order of approximation: $\ell \leftarrow 2m\delta$. (We examine if the equation $\alpha_i^m + \sum_{\mu=0}^{m-1} h_{i,\mu}(Y)\alpha_i^{\mu} \equiv 0 \,(\mathrm{mod}\, Y^{\ell+1})$ has a solution for $h_{i,\mu}(Y) \in K[Y]$ with $\deg(h_{i,\mu}) \leqslant m-\mu$. Writing $h_{i,\mu}(Y) = \sum_{\eta=0}^{m-\mu} u_{i,\mu,\eta} Y^{\eta}$, with $u_{i,\mu,\eta} \in K$, and collecting the coefficients of Y^k we are led to the following problem.)

For $0 \leqslant k \leqslant \ell$, solve the following linear system over K in the variables $u_{i,\mu,\eta}$ $(0 \leqslant \mu \leqslant m-1,\ 0 \leqslant \eta \leqslant m-\mu)$:

$$a_{i,k}^{(m)} + \sum_{\mu=0}^{m-1} \sum_{\eta=0}^{m-\mu} a_{i,k-\eta}^{(\mu)} u_{i,\mu,\eta} = 0 \quad (\text{where } a_{i,v}^{(\mu)} = 0 \text{ for } v < 0), \tag{8}$$

(Since $\deg h_{i,\mu} \leqslant m-\mu$ holds, for every μ we have $m-\mu+1$ indeterminates, which implies that the system has $(m+1)(m+2)/2-1$ indeterminates.)

If (8) *has a solution then*

$$f_i(X,Y) \leftarrow X^m + \sum_{\mu=0}^{m-1} \sum_{\eta=0}^{m-\mu} u_{i,\mu,\eta} Y^\eta X^\mu.$$

(The polynomial $f_i(X,Y)$ is an irreducible factor of $f(X,Y)$ of degree D or some factor of it is an irreducible factor of degree less than D.)

Check if f_i has been produced by a root ζ_l with $l < i$. If not, add f_i to the list of irreducible factors of degree less than D.

If (8) *has no solution for all $i = 1, \ldots, \delta$ and $m = 1, \ldots, D$, then f has no irreducible factors in $K[X,Y]$ of degree at most D.*

The next lemma proves the correctness of this algorithm:

Lemma 3.1. *The polynomial $f(X,Y)$ has an irreducible factor over K of degree at most D if and only if at least one of the $D\delta$ linear systems* (8) *has a solution in K.*

Proof. Suppose that (8) has a solution in K, i.e. there exists $1 \leqslant i \leqslant \delta$ and a polynomial $g_i(X,Y) \in K[X,Y]$ of degree $1 \leqslant m \leqslant D$ such that $g(\alpha_i, Y) \equiv 0 \pmod{Y^{2m\delta+1}}$. Let $\rho \in K[Y]$ denote the resultant $\rho(Y) := \mathrm{Res}_X(f,g)$. Evaluating ρ at $X = \alpha_i$ we conclude that $\rho(Y) \equiv 0 \pmod{Y^{2m\delta+1}}$. Since ρ is a polynomial of degree at most $2m\delta$, we conclude that $\rho = 0$ holds. Hence f and g have a nontrivial common factor in $K[X,Y]$, and therefore f has a factor of degree at most D.

Now, suppose that $f(X,Y)$ has an irreducible factor $g(X,Y) \in K[X,Y]$ of degree at most $D \geqslant 1$. Then there exists a nontrivial factorization $f(X,Y) = g(X,Y)h(X,Y)$ over $K[X,Y]$. Let $1 \leqslant i \leqslant d$ be an integer for which $g(\alpha_{i,0}, 0) = 0$. Then $h(\alpha_{i,0}, 0) \neq 0$, which implies $h(\alpha_{i,0}, Y) \not\equiv 0 \pmod{Y}$ and thus $h(\alpha_{i,j}, Y) \not\equiv 0 \pmod{Y}$ for $1 \leqslant j \leqslant \lfloor \log_2(\ell_{\max}) \rfloor + 1$. Therefore, we have $h(\alpha_i, Y) \not\equiv 0 \pmod{Y}$, which combined with $f(\alpha_i, Y) \equiv 0 \pmod{Y^{2D\delta+1}}$ shows that $g(\alpha_i, Y) \equiv 0 \pmod{Y^{2D\delta+1}}$ holds. We conclude that the coefficients of g, considered as polynomial of $K[Y][X]$, furnish a solution to at least one of the $D\delta$ linear systems (8). This completes the proof. □

3.2. The genericity condition underlying the existence of irreducible components of a given degree

The estimates on the number of q-rational points of a given absolutely irreducible $(n-r)$-dimensional $\mathbb{F}_q$-variety $V \subset \mathbb{A}^n$ of e.g. [Sch76,HW98,CM02] depend strongly on a suitable effective version of the first Bertini theorem. As it is well-known, the first Bertini theorem (see e.g. [Sha94, §II.6.1, Theorem 1]) asserts that the intersection $V \cap L$ of V with a generic affine linear variety $L \subset \mathbb{A}^n$ of dimension $r+1$ is an absolutely irreducible curve. An effective version of the first Bertini theorem aims at estimating the number of planes L for which $V \cap L$ is not an absolutely irreducible curve, and is usually achieved by analyzing the genericity condition underlying the choice of L. The estimates for hypersurfaces we shall present in the next sections rely on a variant of the effective first Bertini theorem, which estimates the number of planes L whose intersection with a given absolutely irreducible $\mathbb{F}_q$-hypersurface H has absolutely irreducible $\mathbb{F}_q$-components of degree at most D for a given $1 \leqslant D \leqslant \delta - 1$.

For this purpose, let $f \in K[X_1, \ldots, X_n]$ be an absolutely irreducible polynomial of degree δ and let be given $1 \leqslant D \leqslant \delta - 1$. For $v_1, \ldots, v_n, \omega_2, \ldots, \omega_n \in \overline{K}$, we consider the polynomial

$$\chi(X, Y, Z_2, \ldots, Z_n) := f(X + v_1, \omega_2 X + Z_2 Y + v_2, \ldots, \omega_n X + Z_n Y + v_n)$$

as an element of $\overline{K}[X, Y, Z_2, \ldots, Z_n]$. Following [Kal95, Lemmas 4 and 5], there exists a nonzero polynomial $\Upsilon \in K[V_1, \ldots, V_n, W_2, \ldots, W_n]$ of degree at most $2\delta^2$ such that for any $v_1, \ldots, v_n, \omega_2, \ldots, \omega_n \in \overline{K}$ with

$$\Upsilon(v_1, \ldots, v_n, \omega_2, \ldots, \omega_n) \neq 0 \tag{9}$$

the following conditions are satisfied:

- the leading coefficient of χ with respect to X is a nonzero element of $\overline{K}$,
- the discriminant of $\chi(X, 0, Z_2, \ldots, Z_n)$ with respect to X is nonzero,
- χ is an irreducible element of $\overline{K}[X, Y, Z_2, \ldots, Z_n]$.

Under the assumption of condition (9), Kaltofen proves a crucial fact for his effective version of the first Bertini theorem [Kal95, Theorem 5]: he shows the existence of a polynomial $\Psi \in \overline{K}[Z_2, \ldots, Z_n]$ of degree at most $3\delta^4/2 - 2\delta^3 + \delta^2/2$ such that for any $\eta := (\eta_2, \ldots, \eta_n) \in \overline{K}^{n-1}$ with $\Psi(\eta) \neq 0$, the bivariate polynomial $\chi(X, Y, \eta_2, \ldots, \eta_n) \in \overline{K}[X, Y]$ is absolutely irreducible.

Hence, for $\Xi := \Upsilon(V_1, \ldots, V_n, W_2, \ldots, W_n)\Psi(Z_2, \ldots, Z_n)$ we have $\deg \Xi \leqslant 3\delta^4/2 - 2\delta^3 + 5\delta^2/2$ and for any $(v, \omega, \eta) := (v_1, \ldots, v_n, \omega_2, \ldots, \omega_n, \eta_2, \ldots, \eta_n) \in \overline{K}^{3n-2}$ with $\Xi(v, \omega, \eta) \neq 0$, the polynomial $\chi(X, Y, \eta_2, \ldots, \eta_n) := f(X + v_1, \omega_2 X + \eta_2 Y + v_2, \ldots, \omega_n X + \eta_n Y + v_n)$ is absolutely irreducible. In particular, for $K = \mathbb{F}_q$ we deduce the following corollary:

Corollary 3.2. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be absolutely irreducible of degree δ. Then there exists at most $(3\delta^4/2 - 2\delta^3 + 5\delta^2/2)q^{3n-3}$ elements $(v, \omega, \eta) \in \mathbb{F}_q^{3n-2}$ for which $\chi(X, Y, \eta)$ is not absolutely irreducible.*

Our goal is to obtain a degree estimate, similar to that of deg Ξ, on the genericity condition underlying the nonexistence of absolutely irreducible factors of $\chi(X, Y, \eta_2, \ldots, \eta_n)$ of degree at most D for a given $1 \leqslant D \leqslant \delta - 1$. Our next theorem, a variant of Kaltofen [Kal95, Theorem 5], will be a crucial point for our estimates of the following sections.

Theorem 3.3. *Let $1 \leqslant D \leqslant \delta - 1$ and suppose that $v_1, \ldots, v_n, \omega_2, \ldots, \omega_n$ satisfy condition* (9). *Then there exists a nonzero polynomial $\Psi_D \in \overline{K}[Z_2, \ldots, Z_n]$ of degree*

$$\deg \Psi_D \leqslant D\delta^2(D+1)(D+2) - (D^2+3D)(D^2+3D+2)\delta/8$$

such that for any $\eta := (\eta_2, \ldots, \eta_n) \in \overline{K}^{n-1}$ with $\Psi_D(\eta) \neq 0$, the polynomial $\chi(X, Y, \eta) := f(X + v_1, \omega_2 X + \eta_2 Y + v_2, \ldots, \omega_n X + \eta_n Y + v_n)$ has no irreducible factors of degree at most D in $\overline{K}[X, Y]$.

Proof. Since by assumption χ is irreducible over $\overline{K}[Z_2, \ldots, Z_n][X, Y]$, Gauss Lemma implies that χ is irreducible over $\overline{K}(Z_2, \ldots, Z_n)[X, Y]$. Therefore, applying algorithm *Factorization over the Coefficient Field of degree at most D* to the polynomial $\psi := l^{-1}\chi \in \overline{K}(Z_2, \ldots, Z_n)[X, Y]$, where $l \in \overline{K}$ is the leading coefficient of χ, since $\psi(X, 0) \in \overline{K}[X]$, the root ζ_i used to construct the field $K_i := K(\zeta_i)$ of the algorithm is actually an element of $\overline{K}$ for $1 \leqslant i \leqslant \delta$. Then the irreducibility of ψ over $\overline{K}(Z_2, \ldots, Z_n)[X, Y]$ implies that the linear system (8) derived in step L has no solution in the field K_i for $1 \leqslant m \leqslant D$ and $1 \leqslant i \leqslant \delta$. This implies that for $m = D$ and $1 \leqslant i \leqslant \delta$, the augmented matrix of the system, $\widetilde{M}_D^{(i)}(Z_2, \ldots, Z_n)$, has rank greater than that of the matrix of the coefficients $M_D^{(i)}(Z_2, \ldots, Z_n)$. Since $\partial\psi(X, 0)/\partial X \in \overline{K}$, all the denominators used in the construction of this system are elements of $\overline{K}$. Let $\Psi_D^{(i)} \in \overline{K}[Z_2, \ldots, Z_n]$ be a maximal nonzero minor of the augmented matrix $\widetilde{M}_D^{(i)}(Z_2, \ldots, Z_n)$ and let $\eta := (\eta_2, \ldots, \eta_n) \in \overline{K}^{n-1}$ satisfy $\prod_{i=1}^{\delta} \Psi_D^{(i)}(\eta) \neq 0$. Then the specialized system (8) has no solutions for $i = 1, \ldots, \delta$, which implies that $\chi(X, Y, \eta_2, \ldots, \eta_n)$ has no irreducible factors over $\overline{K}[X, Y]$ of degree at most D, because algorithm *Factorization over the Coefficient Field of degree at most D* fails to find such a factor of $\chi(X, Y, \eta)$ over $\overline{K}$. Therefore, $\Psi_D := \prod_{i=1}^{\delta} \Psi_D^i$ is the polynomial we are looking for.

Now we show that the degree estimate for Ψ_D holds. The degree estimate essentially follows from the proof of Kaltofen [Kal95, Theorem 5], taking into account that we have a different number of indeterminates and a different order of approximation. Indeed, for every root ζ_i of $\psi(x, 0)$, the corresponding linear system for $m = D$ has $(D+1)(D+2)/2 - 1$ indeterminates. Hence, any maximal nonzero minor $\Psi_D^{(i)}$ satisfies

the following degree estimate:

$$\begin{aligned}\deg_{Z_2,\ldots,Z_n} \Psi_D^{(i)} &\leqslant \sum_{j=0}^{(D+1)(D+2)/2-1} (\ell_{\max} - j)\\ &\leqslant 2D\delta(D+1)(D+2)/2 - (D^2+3D)(D^2+3D+2)/8.\end{aligned}$$

This immediately implies the degree estimate for Ψ_D of the theorem. □

Since Theorem 3.3 is valid under the assumption of condition (9), if we define

$$\Xi_D := \Upsilon(V_1, \ldots, V_n, W_2, \ldots, W_n)\Psi_D(Z_2, \ldots, Z_n),$$

then Ξ_D is a polynomial in $3n-2$ indeterminates with coefficients in $\overline{K}$ of degree bounded by

$$\deg \Xi_D \leqslant D^3\delta^2 - D^4\delta/8 - 3D^3\delta/4 + 3D^2\delta^2 - 11D^2\delta/8 + 2D\delta^2 - 3D\delta/4 + 2\delta^2,$$

which satisfies the following property: for every $(v, \omega, \eta) \in \overline{K}^{3n-2}$ with $\Xi_D(v, \omega, \eta) \neq 0$, the polynomial $\chi(X, Y, \eta_2, \ldots, \eta_n)$ has no irreducible factors over $\overline{K}$ of degree at most D. Therefore, for $K = \mathbb{F}_q$ we have the following corollary:

Corollary 3.4. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an absolutely irreducible polynomial of degree $\delta \geqslant 2$ and let be given an integer D with $1 \leqslant D \leqslant \delta - 1$. Then there are at most $(D^3\delta^2 - D^4 d/8 - 3D^3\delta/4 + 3D^2\delta^2 - 11D^2\delta/8 + 2D\delta^2 - 3D\delta/4 + 2\delta^2)q^{3n-3}$ elements $(v, \omega, \eta) \in \mathbb{F}_q^{3n-2}$ for which $\chi(X, Y, \eta_2, \ldots, \eta_n)$ has an irreducible factor over $\overline{\mathbb{F}}_q[X, Y]$ of degree at most D.*

4. On the intersection of an absolutely irreducible $\mathbb{F}_q$-hypersurface with an $\mathbb{F}_q$-plane

Following [Sch74], in this section we estimate, for a given polynomial f, the number of planes L for which the restriction of f to L has a fixed number of absolutely irreducible $\mathbb{F}_q$-factors. For this purpose, we shall consider the results from the previous section from a geometric point of view. We shall work with the field $K := \mathbb{F}_q$ and every nonzero $(v, \omega, \eta) \in \mathbb{F}_q^{3n-2}$ shall be considered as providing a parametrization of a linear affine $\mathbb{F}_q$-variety of $\mathbb{A}^n$ of dimension 2.

More precisely, let be given a polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree $\delta > 0$. For an affine linear $\mathbb{F}_q$-variety $L \subset \mathbb{A}^n$ of dimension 2 (an $\mathbb{F}_q$-plane for short), we represent the restriction of f to L as a bivariate polynomial $f_L \in \mathbb{F}_q[X, Y]$, where X, Y are the parameters of a given parametrization of L. Let us remark that for every such L, the polynomial f_L is univocally defined up to an $\mathbb{F}_q$-definable affine linear change of coordinates. Therefore, its degree and number of absolutely irreducible components

do not depend on the particular parametrization of L we choose to represent L (cf. [Sch76, V.§4]).

In particular, we shall be concerned with the $\mathbb{F}_q$-planes of $\mathbb{A}^n$ which have an $\mathbb{F}_q$-definable parametrization of the following type:

$$X_1 = v_1 + X, \qquad X_i = v_i + \omega_i X + \eta_i Y \quad (2 \leqslant i \leqslant n). \tag{10}$$

Let $M_T^{(2)}$ denote the set of all $\mathbb{F}_q$-planes of $\mathbb{A}^n$ and let $M^{(2)}$ denote the subset formed by the elements of $M_T^{(2)}$ having a parametrization as in (10).

Our purpose is to analyze the number of absolutely irreducible factors of f_L for a given $\mathbb{F}_q$-plane $L \subset \mathbb{A}^n$. Hence, for a plane $L \in M^{(2)}$ on which f does not vanish identically, we denote by $\nu(L)$ the number of absolutely irreducible $\mathbb{F}_q$-factors of f_L. Then $0 \leqslant \nu(L) \leqslant \delta$ if f does not vanish identically on L and we define $\nu(L) := q$ otherwise. Further, let Π_j be the set of planes L with $|\nu(L) - 1| = j$. Thus, Π_1 is the set of planes L with 0 or 2 absolutely irreducible $\mathbb{F}_q$-factors, Π_j is the set of planes L for which f_L has $j+1$ absolutely irreducible $\mathbb{F}_q$-factors for $j = 0, 2, \ldots, \delta - 1$, and Π_{q-1} is the set of planes L for which f_L vanishes identically.

Observe that if $L \in \Pi_j$ for a given $j = 0, \ldots, \delta - 1$ then f_L has an absolutely irreducible factor of degree at most $D_j := \lfloor \delta/(j+1) \rfloor$. Theorem 3.3 asserts that for any plane $L \in M^{(2)}$ having an $\mathbb{F}_q$-parametrization as in (10) with $\Xi_{D_j}(v, \omega, \eta) \neq 0$, the polynomial f_L has no irreducible factors over $\overline{\mathbb{F}}_q$ of degree at most D_j. Therefore, for every such $(v, \omega, \eta) \in \mathbb{F}_q^{3n-2}$, f_L has at most j irreducible factors over $\overline{\mathbb{F}}_q$, which in particular implies that $L \notin \Pi_j \cup \cdots \cup \Pi_{\delta-1}$ holds. Hence any $L \in \Pi_j \cup \cdots \Pi_{\delta-1}$ has a parmetrization as in (10) with

$$\{(v, \omega, \eta) \in \mathbb{F}_q^{3n-2} : \Xi_{D_j}(v, \omega, \eta) = 0\}.$$

Taking into account that every plane of $M^{(2)}$ has $q^3(q-1)$ $\mathbb{F}_q$-parametrizations as in (10), from Lemma 2.1 we deduce the following estimate:

$$\#(\Pi_j) + \cdots + \#(\Pi_{\delta-1}) \leqslant \deg \Xi_{D_j} \frac{q^{3n-3}}{q^3(q-1)}.$$

Therefore, from Corollary 3.4 we obtain

$$\sum_{k=j}^{\delta-1} \#(\Pi_k) \leqslant \left(\delta^5 \left(\frac{1}{j^3} - \frac{1}{8j^4} \right) + 3\delta^4 \left(\frac{1}{j^2} - \frac{1}{4j^3} \right) + \delta^3 \left(\frac{2}{j} - \frac{11}{8j^2} \right) - \frac{3}{4}\frac{\delta^2}{j} + 2\delta^2 \right) \frac{q^{3n-6}}{(q-1)}. \tag{11}$$

The following proposition is crucial for our estimates for an absolutely irreducible $\mathbb{F}_q$-hypersurface of the next section. It yields a better estimate than that obtained by a straightforward application of Corollary 3.2.

Proposition 4.1. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a polynomial of degree $\delta > 1$. Then the following estimate holds*:

$$\sum_{j=1}^{\delta-1} j\#(\Pi_j) \leqslant (2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}}) \frac{q^{3n-3}}{q^3(q-1)}.$$

Proof. For $\delta = 2$ the expression $\sum_{j=1}^{\delta-1} j\#(\Pi_j)$ consists of only one term, namely Π_1, and therefore Corollary 3.2 yields

$$\#(\Pi_1) \leqslant \left(\frac{3}{2}\delta^4 - 2\delta^3 + \frac{5}{2}\delta^2\right) \frac{q^{3n-6}}{(q-1)} \leqslant \frac{3}{2}\delta^4 \frac{q^{3n-6}}{(q-1)}. \tag{12}$$

Hence, we may assume without loss of generality $\delta \geqslant 3$. Let r be a real number, to be fixed below, lying in the open real interval $(1, \delta - 1)$. We have

$$\begin{aligned} \sum_{j=1}^{\delta-1} j\#(\Pi_j) &= \sum_{j=1}^{\lfloor r \rfloor} j\#(\Pi_j) + \sum_{j=\lfloor r \rfloor+1}^{\delta-1} j\#(\Pi_j) \\ &\leqslant \lfloor r \rfloor \sum_{j=1}^{\delta-1} \#(\Pi_j) + \sum_{j=\lfloor r \rfloor+1}^{\delta-1} (j - \lfloor r \rfloor)\#(\Pi_j). \end{aligned}$$

By Corollary 3.2 we have

$$\lfloor r \rfloor \sum_{j=1}^{\delta-1} \#(\Pi_j) \leqslant r \left(\frac{3}{2}\delta^4 - 2\delta^3 + \frac{5}{2}\delta^2\right) \frac{q^{3n-6}}{(q-1)}. \tag{13}$$

On the other hand, by inequality (11) we have

$$\begin{aligned} \sum_{j=\lfloor r \rfloor+1}^{\delta-1} (j - \lfloor r \rfloor)\#(\Pi_j) &= \sum_{j=\lfloor r \rfloor+1}^{\delta-1} (\#(\Pi_j) + \cdots + \#(\Pi_{\delta-1})) \\ &\leqslant \left(\delta^5 c_1 + 3\delta^4 c_2 + \delta^3 c_3 - \frac{3}{4}\delta^2 c_4 + 2\delta^2\right) \frac{q^{3n-6}}{(q-1)}, \end{aligned} \tag{14}$$

where c_1, c_2, c_3, c_4 are the following numbers:

$$c_1 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{1}{j^3} - \frac{1}{8j^4}, \quad c_2 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{1}{j^2} - \frac{1}{4j^3},$$

$$c_3 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{2}{j} - \frac{11}{8j^2}, \quad c_4 := \sum_{j=\lfloor r\rfloor+1}^{\delta-1} \frac{1}{j}.$$

We observe that any decreasing positive real function g satisfies the inequality $\sum_{j=\lfloor r\rfloor+1}^{\delta-1} g(j) \leqslant \int_r^{\delta-1} g(x)\,dx$. Let $r := \delta^{\frac{1}{3}}$. Using the fact that $1 < \delta/(\delta-1) \leqslant \frac{3}{2}$ holds for $\delta \geqslant 3$, we have the following inequalities:

$$\begin{aligned}
\delta^5 c_1 &\leqslant \delta^5 \left(\tfrac{1}{2}(\delta^{\frac{1}{3}})^{-2} - \tfrac{1}{24}(\delta^{\frac{1}{3}})^{-3} - \tfrac{1}{2}(\delta-1)^{-2} + \tfrac{1}{24}(\delta-1)^{-3}\right) \\
&\leqslant \tfrac{1}{2}\delta^{\frac{13}{3}} - \tfrac{1}{24}\delta^4 - \tfrac{1}{2}\delta^3 + \tfrac{9}{64}\delta^2, \\
3\delta^4 c_2 &\leqslant 3\delta^4 \left(\delta^{-\frac{1}{3}} - \tfrac{1}{8}(\delta^{\frac{1}{3}})^{-2} - (\delta-1)^{-1} + \tfrac{1}{8}(\delta-1)^{-2}\right) \\
&\leqslant 3\delta^{\frac{11}{3}} - \tfrac{3}{8}\delta^{\frac{10}{3}} - 3\delta^3 + \tfrac{27}{32}\delta^2, \\
\delta^3 c_3 &\leqslant \delta^3(2\ln(\delta-1) + \tfrac{11}{8}(\delta-1)^{-1} - 2\ln\delta^{\frac{1}{3}} - \tfrac{11}{8}\delta^{-\frac{1}{3}}) \\
&\leqslant \tfrac{4}{3}\delta^3 \ln\delta + \tfrac{33}{16}\delta^2 - \tfrac{11}{8}\delta^{\frac{8}{3}}.
\end{aligned}$$

This implies that the following estimate holds:

$$\begin{aligned}
&\delta^5 c_1 + 3\delta^4 c_2 + \delta^3 c_3 - \tfrac{3}{4}\delta^2 c_4 + 2\delta^2 \\
&\quad \leqslant \tfrac{1}{2}\delta^{\frac{13}{3}} - \tfrac{1}{24}\delta^4 + 3\delta^{\frac{11}{3}} - \tfrac{3}{8}\delta^{\frac{10}{3}} + \tfrac{4}{3}\delta^3 \ln\delta - \tfrac{7}{2}\delta^3 - \tfrac{11}{8}\delta^{\frac{8}{3}} + \tfrac{323}{64}\delta^2. \qquad (15)
\end{aligned}$$

Now, putting together (13)–(15), and taking into account that $\frac{4}{3}\delta^3 \ln\delta \leqslant 3\delta^{3+1/3}$ holds for $\delta \geqslant 3$, we obtain

$$\begin{aligned}
\sum_{j=1}^{\delta-1} j\#(\Pi_j) &\leqslant 2\delta^{\frac{13}{3}} - \tfrac{1}{24}\delta^4 + 3\delta^{\frac{11}{3}} + \tfrac{5}{8}\delta^{\frac{10}{3}} - \tfrac{7}{2}\delta^3 - \tfrac{11}{8}\delta^{\frac{8}{3}} + \tfrac{5}{2}\delta^{\frac{7}{3}} + \tfrac{323}{64}\delta^2 \\
&\leqslant 2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}}
\end{aligned}$$

for $\delta \geqslant 3$. This proves the proposition. □

5. Estimates for an absolutely irreducible $\mathbb{F}_q$-hypersurface

In this section, we obtain different types of estimates on the number of q-rational points of a given absolutely irreducible $\mathbb{F}_q$-hypersurface. First, we exhibit an estimate which holds without any regularity condition and improves (4) and (6). Then, we show an estimate which improves both the right-hand side and the regularity condition of the lower bound (5), providing also a corresponding upper bound. Finally, we extend these estimates to the case of an arbitrary $\mathbb{F}_q$-hypersurface.

For this purpose, we shall follow an approach that combines both ideas of Schmidt [Sch74,Sch76] with the estimate of the previous section. This approach is based on estimating the number of q-rational points lying in the intersection of a given absolutely irreducible $\mathbb{F}_q$-hypersurface with all the $\mathbb{F}_q$-planes of $\mathbb{A}^n$.

5.1. An estimate without any regularity condition

In what follows, we shall apply the following lemma from [Sch74].

Lemma 5.1 (*[Sch74, Lemma 5]*). *Let $f \in \mathbb{F}_q[X, Y]$ be a polynomial of degree $\delta > 0$ and let v be the number of distinct absolutely irreducible $\mathbb{F}_q$-factors of f. Then the number N of zeros of f in $\mathbb{F}_q^2$ satisfies*

$$|N - vq| \leqslant \omega(q, \delta) + \delta^2,$$

where $\omega(q, \delta) := (\delta - 1)(\delta - 2)q^{1/2} + \delta + 1$.

Let be given an absolutely irreducible polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree $\delta > 0$. Recall that $M_T^{(2)}$ and $M^{(2)}$ denote the set of $\mathbb{F}_q$-planes of $\mathbb{A}^n$ and the set of $\mathbb{F}_q$-planes with a parametrization as in (10), respectively. Further, for $j = 0, 2, \ldots, \delta - 1$ let Π_j be the set of $\mathbb{F}_q$-planes $L \in M^{(2)}$ for which the restriction f_L of f to L has $j+1$ absolutely irreducible $\mathbb{F}_q$-definable factors, let Π_1 be the set of $\mathbb{F}_q$-planes $L \in M^{(2)}$ for which f_L has 0 or 2 absolutely irreducible $\mathbb{F}_q$-factors, and let Π_{q-1} denote the set of $\mathbb{F}_q$-planes $L \in M^{(2)}$ for which f_L vanishes identically. Let us introduce the following quantities:

$$A := \# M^{(2)}, \qquad B := \sum_{j=1}^{\delta-1} j\#(\Pi_j), \qquad C := \#(\Pi_{q-1}), \qquad D := \#M_T^{(2)} - \#M^{(2)}.$$

Let E denote the number of elements of $M_T^{(2)}$ containing a given point of $\mathbb{F}_q^n$.

We recall that any element of $M^{(2)}$ is represented by $D' := q^3(q-1)$ different parametrizations of type (10). Therefore, taking into account that there are

$q^{2n-1}(q^{n-1}-1)$ different parametrizations of type (10), we conclude that

$$A = \frac{q^{2n-1}(q^{n-1}-1)}{q^3(q-1)} \tag{16}$$

holds. By Proposition 4.1 we have $B \leqslant (2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}})\frac{q^{3n-3}}{q^3(q-1)}$, which implies

$$\frac{B}{A} \leqslant \left(2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}}\right)\frac{q^{n-2}}{q^{n-1}-1}. \tag{17}$$

By a simple recursive argument we may assume without loss of generality that f cannot be expressed as a polynomial in $n-2$ variables (see e.g. [Sch76]). Let us fix $c \in \mathbb{F}_q^{n-2}$ for which $f(c, X_{n-1}, X_n)$ vanishes identically. Let us write $f = \sum_{\alpha\in\mathcal{J}} f_\alpha X_{n-1}^{\alpha_1} X_n^{\alpha_2}$, where $\mathcal{J} \subset (\mathbb{Z}_{\geqslant 0})^2$ is a suitable finite set and $f_\alpha \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$ for any $\alpha = (\alpha_1, \alpha_2) \in \mathcal{J}$. Since f is not a polynomial of $\mathbb{F}_q[X_1, \ldots, X_{n-2}]$, it follows that $f_\alpha(c) = 0$ for any $\alpha \in \mathcal{J}$. By the absolute irreducibility of f we have that the set of polynomials $\{f_\alpha : \alpha \in \mathcal{J}\} \subset \mathbb{F}_q[X_1, \ldots, X_{n-2}]$ does not have nontrivial common factors in $\overline{\mathbb{F}}_q[X_1, \ldots, X_{n-2}]$. Then Lemma 2.2 implies that there exist at most $\delta^2 q^{n-4}$ elements $c \in \mathbb{F}_q^{n-2}$ for which $f(c, X_{n-1}, X_n) = 0$ holds, and hence there exist at most $\delta^2 q^{n-4}$ linear varieties L of M_2 parallel to $X_1 = 0, \ldots, X_{n-2} = 0$ for which $f_L = 0$ holds. Let A_0 denote the number of different subspaces belonging to $M^{(2)}$. Repeating this argument for all the subspaces of $M^{(2)}$ we obtain

$$\frac{C}{A} \leqslant \frac{\delta^2 q^{n-4} A_0}{q^{n-2} A_0} = \frac{\delta^2}{q^2}. \tag{18}$$

Let us observe that $\#M_T^{(2)} = q^n(q^n-1)(q^n-q)/\big(q^2(q^2-1)(q^2-q)\big)$. Combining this observation with (16) we have

$$\frac{D}{A} = \frac{1}{A}(\#M_T^{(2)} - A) = \frac{1}{A}\,\frac{q^n(q^{n-1}-1)(q^{n-1}-q)}{q^2(q^2-1)(q^2-q)} \leqslant \frac{4}{3q^2}. \tag{19}$$

Let us fix a point $x \in \mathbb{F}_q^n$. Then there are $E = (q^n-1)(q^n-q)/\big((q^2-1)(q^2-q)\big)$ varieties $L \in M_T^{(2)}$ passing through x. This implies

$$\frac{A}{E} \leqslant q^{n-2}. \tag{20}$$

Now we are ready to state our estimate for hypersurfaces *without any regularity condition*.

Theorem 5.2. *For an absolutely irreducible $\mathbb{F}_q$-hypersurface H of $\mathbb{A}^n$ of degree δ the following estimate holds*:

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{\frac{13}{3}} q^{n-2}.$$

Proof. First we observe that the theorem is obviously true if $\delta = 1$. Therefore, we may assume without loss of generality $\delta \geqslant 2$.

Let $N := \#(H \cap \mathbb{F}_q^n)$. With the notations introduced before, we have

$$|N - q^{n-1}| \leqslant \frac{1}{E}\left(\sum_{L\in M^{(2)}} |N(f_L) - q| + \sum_{L\in M_T^{(2)}\setminus M^{(2)}} |N(f_L) - q|\right). \tag{21}$$

In order to estimate the first term of the right-hand side of (21), for a plane $L \in \Pi_j$ with $j \in \{0,\dots,\delta-1\}$, Lemma 5.1 implies $|N(f_L) - q| \leqslant |N(f_L) - v(L)q| + |v(L) - 1|q \leqslant \omega(q,\delta) + \delta^2 + jq$. Therefore, we have:

$$\begin{aligned}
\sum_{L\in M^{(2)}} |N(f_L) - q| &\leqslant \sum_{j=0}^{\delta-1}\left(\sum_{L\in\Pi_j}\big(\omega(q,\delta)+\delta^2+jq\big)\right) + \sum_{L\in\Pi_{q-1}}(q^2-q)\\
&\leqslant \left(\sum_{j=0}^{\delta-1}\#(\Pi_j)\right)\big(\omega(q,\delta)+\delta^2\big) + q\sum_{j=1}^{q-1} j\#(\Pi_j)\\
&\leqslant A(\omega(q,\delta)+\delta^2) + Bq + Cq(q-1).
\end{aligned}$$

Replacing this inequality in (21) and taking into account (17)–(20) we obtain for $\delta \geqslant 3$

$$\begin{aligned}
|N - q^{n-1}| &\leqslant \frac{1}{E}\big(A(\omega(q,\delta)+\delta^2) + Bq + Cq(q-1) + Dq^2\big)\\
&\leqslant \frac{A}{E}\left(\omega(q,\delta)+\delta^2 + \frac{B}{A}q + \frac{C}{A}q(q-1) + \frac{D}{A}q^2\right)\\
&\leqslant q^{n-2}\big(\omega(q,\delta)+\delta^2 + (2\delta^{\frac{13}{3}} + 3\delta^{\frac{11}{3}})\tfrac{4}{3} + \delta^2 + \tfrac{4}{3}\big)\\
&\leqslant (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{\frac{13}{3}} q^{n-2}.
\end{aligned} \tag{22}$$

For $\delta = 2$, combining (21) with estimate (12) of the proof of Proposition 4.1, we obtain

$$\begin{aligned}
|N - q^{n-1}| &\leqslant q^{n-2}\big(\omega(q,\delta)+\delta^2 + \big(\tfrac{3}{2}\delta^4 - 2\delta^3 + \tfrac{5}{2}\delta^2\big)\tfrac{4}{3} + \delta^2 + \tfrac{4}{3}\big)\\
&\leqslant (\delta-1)(\delta-2)q^{n-3/2} + (2\delta^4 + 3\delta)q^{n-2}\\
&\leqslant (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{\frac{13}{3}} q^{n-2}.
\end{aligned} \tag{23}$$

This finishes the proof of the theorem. □

Observe that our estimate holds with no restriction on q and clearly improves the previous record estimate (up to the authors knowledge), due to [HW98], which is only valid for $q > cn^3\delta^5 \log^3 \delta$:

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + (2\delta^5 + \delta^2)q^{n-2} + 2\delta^7 q^{n-5/2}.$$

Moreover, we also improve the estimate of Ghorpade and Lachaud [GL02a,GL02b]. We recall that in the case of a hypersurface the estimate is

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + 12(\delta+3)^{n+1}q^{n-2}.$$

In [CR96], the authors show that for q sufficiently large the following assertions hold (see [CR96, Theorem 3.2 and 3.4]) for any polynomial $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree $\delta > 1$:

(i) if f is absolutely irreducible, then $\#\big(V(f) \cap \mathbb{F}_q^n\big) < \delta q^{n-1} - (\delta-1)q^{n-2}$,
(ii) if f has an absolutely irreducible nonlinear $\mathbb{F}_q$-definable factor, then $\#\big(V(f) \cap \mathbb{F}_q^n\big) < \delta q^{n-1} - (\delta-1)q^{n-2}$.

Further, they ask whether the previous assertions hold for any q. Although we are not able to answer this question, our estimates provide explicit values $q_0 = q_0(\delta)$ and $q_1 = q_1(\delta)$ such that (i) holds for $q \geqslant q_0$ and (ii) holds for $q \geqslant q_1$. Indeed, Theorem 5.2 implies that we may choose $q_0 := 13\delta^{\frac{10}{3}}$ and $q_1 := 9\delta^{\frac{13}{3}}$.

5.2. An improved estimate with regularity condition

In this section, we are going to exhibit an estimate on the number of q-rational points of an absolutely irreducible $\mathbb{F}_q$-variety which improves that of Theorem 5.2 but is only valid under a certain regularity condition.

Theorem 5.3. *Let $q > 15\delta^{\frac{13}{3}}$ and let $H \subset \mathbb{A}^n$ be an absolutely irreducible $\mathbb{F}_q$-hypersurface of degree δ. Then the following estimate holds*:

$$|\#(H \cap \mathbb{F}_q^n) - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + (5\delta^2 + \delta + 1)q^{n-2}.$$

Proof. Let $N := \#(H \cap \mathbb{F}_q^n)$. Since the statement of the theorem is obviously true for $\delta = 1$, we may assume without loss of generality that $\delta \geqslant 2$ holds.

With notations as before, for a plane $L \in \Pi_j$ with $j > 0$ it follows by Lemma 5.1 that $|N(f_L) - q| < jq + \omega(q,\delta) + \delta^2$ holds. Therefore, we have

$$\begin{aligned} |N(f_L) - Nq^{2-n}| &\geqslant |N(f_L) - q| - q^{2-n}|N - q^{n-1}| \\ &\geqslant jq - \omega(q,\delta) - \delta^2 - \omega(q,\delta) - 5\delta^{\frac{13}{3}} \\ &\geqslant \tfrac{1}{2}jq, \end{aligned}$$

where the last inequality is valid if and only if $\frac{1}{2}jq \geqslant 2q^{1/2}(\delta-1)(\delta-2)+2(\delta+1)+\delta^2+5\delta^{\frac{13}{3}}$ holds. Hence, our assumption on q implies the validity of the inequality.

From [Sch74, Lemma 6] we have $\frac{1}{4}q^2\sum_{j=1}^{q-1} j^2\#(\Pi_j) \leqslant \delta E q^{n-1}$, which implies $\sum_{j=1}^{q-1} j\#(\Pi_j) \leqslant 4\delta E q^{n-3}$. Hence,

$$\begin{aligned}
|N-q^{n-1}| &= \frac{1}{E}\left|\sum_{L\in M_T^{(2)}}\big(N(f_L)-q\big)\right| \leqslant \frac{1}{E}\sum_{L\in M_T^{(2)}}|(N(f_L)-q)| \\
&\leqslant \frac{1}{E}\left((A+D)\big(\omega(q,\delta)+\delta^2\big)+\sum_{j=1}^{q-1}2jq\#(\Pi_j)\right) \\
&\leqslant q^{n-2}\big(\omega(q,\delta)+\delta^2+8\delta\big) \\
&\leqslant q^{n-2}\big(\omega(q,\delta)+5\delta^2\big).
\end{aligned}$$

This finishes the proof of the theorem. □

From this estimate we deduce the following (nontrivial) lower bound: for $q > 15\delta^{\frac{13}{3}}$, we have

$$N > q^{n-1}-(\delta-1)(\delta-2)q^{n-\frac{3}{2}}-(5\delta^2+\delta+1)q^{n-2}.$$

Therefore, our estimate significantly improves the regularity condition $q > 10^4 n^3\delta^5\vartheta^3([4\log\delta])$ of Schmidt [Sch74], where [ ] denotes integer part and $\vartheta(j)$ is the jth prime, and also provides a corresponding upper bound, not given in [Sch74].

Let us observe that, in the setting of polynomial equation solving over finite fields, lower bounds on the number of q-rational points of a given absolutely irreducible $\mathbb{F}_q$-hypersurface H, such as those underlying Theorems 5.2 and 5.3 or [Sch74], are typically required in order to assure the existence of a q-rational point of H (see e.g. [HW98,HW99,CM03]). Indeed, from [Sch74] one deduces that an absolutely irreducible $\mathbb{F}_q$-hypersurface of degree δ has a q-rational point for $q > 10^4 n^3\delta^5\vartheta^3([4\log\delta])$. Furthermore, from Theorem 5.2 we conclude that this condition can be improved to $q > 9\delta^{\frac{13}{3}}$. Nevertheless, the following simple argument allows us to significantly improve the latter (compare [CM03, Section 6.1]):

Theorem 5.4. *For $q > 2\delta^4$, any absolutely irreducible $\mathbb{F}_q$-hypersurface of degree δ has a q-rational point.*

Proof. Let $H \subset \mathbb{A}^n$ be an absolutely irreducible $\mathbb{F}_q$-hypersurface of degree δ, and let $f \in \mathbb{F}_q[X_1,\ldots,X_n]$ be the defining polynomial of H. Since $q > 2\delta^4$, from Corollary 3.2 we conclude that there exists $(v,\omega,\eta) \in \mathbb{F}_q^{3n-2}$ for which $\chi(X,Y) := f(X+v_1,\omega_2 X+$

$\eta_2 Y + v_2, \ldots, \omega_n X + \eta_n Y + v_n)$ is absolutely irreducible of degree δ. Therefore, Weil's estimate (1) shows that χ has at least $q - (\delta-1)(\delta-2)q^{\frac{1}{2}} - \delta - 1$ q-rational zeros. Since this quantity is a strictly positive real number for $q > 2\delta^4$, we conclude that χ has at least one q-rational zero, which implies that H has at least one q-rational point. □

Finally, we observe that in the case that the characteristic p of the field $\mathbb{F}_q$ is large enough, the estimates of Theorems 5.2 and 5.3 can be further improved, using an effective version of the first Bertini theorem due to Gao [Gao03]. From [Gao03, Theorem 5.1] we deduce the following result:

Corollary 5.5. *Suppose that the characteristic p of $\mathbb{F}_q$ satisfies the condition $p > 2\delta^2$. Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be an absolutely irreducible polynomial of degree $\delta > 1$. Then there are at most $\frac{3}{2}\delta^3 \frac{q^{3n-3}}{q^3(q-1)}$ $\mathbb{F}_q$-planes $L \subset \mathbb{A}^n$ such that the restriction f_L of f to L is not absolutely irreducible.*

With the notations of Section 5.1, from Corollary 5.5 we obtain

$$\frac{B}{A} := \frac{1}{A}\sum_{j=1}^{\delta-1} j\#\Pi_j \leqslant \frac{\delta}{A}\sum_{j=1}^{\delta-1}\#\Pi_j \leqslant \frac{3}{2}\frac{\delta^4}{A}\frac{q^{3n-3}}{q^3(q-1)} \leqslant \frac{3}{2}\,\delta^4\frac{q^{n-2}}{q^{n-1}-1}.$$

Combining this estimate with (22) of the proof of Theorem 5.2, we obtain the following estimate on the number N of q-rational points of any absolutely irreducible hypersurface $H \subset \mathbb{A}^n$ of degree δ

$$|N - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + 3\delta^4 q^{n-2}.$$

Furthermore, replacing in the proof of Theorem 5.3 the lower bound obtained from Theorem 5.2 by the one arising from the above estimate, we obtain for $q > 27\delta^4$

$$|N - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + (5\delta^2+\delta+1)q^{n-2}.$$

Summarizing, we have

Corollary 5.6. *Suppose that $p > 2\delta^2$ holds, and let $H \subset \mathbb{A}^n$ be an absolutely irreducible $\mathbb{F}_q$-hypersurface of degree $\delta > 1$. Then the following estimate holds*:

$$|N - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + 3\delta^4 q^{n-2}.$$

Furthermore, if in addition we have $q > 27\delta^4$, then

$$|N - q^{n-1}| \leqslant (\delta-1)(\delta-2)q^{n-3/2} + (5\delta^2+\delta+1)q^{n-2}.$$

These estimates certainly improve those of Theorems 5.2 and 5.3 for $p > 2\delta^2$, but fail to improve the existence result of Theorem 5.4. Indeed, Corollary 5.6 does not yield a nontrivial lower bound on the number of q-rational points of H for $q \leqslant 4\delta^4$. In fact, taking into account that estimates like of those of Theorems 5.2 and 5.3 and Corollary 5.6 will fail to provide nontrivial lower bounds for $q \leqslant (\delta-1)^2(\delta-2)^2$, we conclude that our existence result of Theorem 5.4 comes quite close to this optimal value.

5.3. An estimate for an arbitrary $\mathbb{F}_q$-hypersurface

We finish our discussion on estimates on the number of q-rational points of an $\mathbb{F}_q$-hypersurface by considering the case of an arbitrary $\mathbb{F}_q$-hypersurface. Nevertheless, it must be remarked that our estimate in the case of an $\mathbb{F}_q$-hypersurface without absolutely irreducible $\mathbb{F}_q$-definable components reduces essentially to Lemma 2.3.

Theorem 5.7. *Let $H \subset \mathbb{A}^n$ $(n \geqslant 2)$ be an $\mathbb{F}_q$-hypersurface of degree δ. Let $H = H_1 \cup \cdots \cup H_\sigma \cup H_{\sigma+1} \cup \cdots \cup H_m$ be the decomposition of H into $\mathbb{F}_q$-irreducible components, where $H_1, \ldots, H_\sigma$ are absolutely irreducible and $H_{\sigma+1}, \ldots, H_m$ are not absolutely irreducible. Let $\delta_i := \deg H_i$ for $1 \leqslant i \leqslant m$ and let $\Delta := \sum_{i=1}^{\sigma} \delta_i$. Then we have the estimate*

$$|\#(H \cap \mathbb{F}_q^n) - \sigma q^{n-1}| \leqslant \operatorname{sign}(\sigma)(\Delta-1)(\Delta-2)q^{n-\frac{3}{2}} + (5\Delta^{\frac{13}{3}} + \delta^2/2)q^{n-2},$$

where $\operatorname{sign}(\sigma) := 0$ *for* $\sigma = 0$ *and* $\operatorname{sign}(\sigma) := 1$ *otherwise.*

Proof. Let $N := \#(H \cap \mathbb{F}_q^n)$ and $N_i := \#(H_i \cap \mathbb{F}_q^n)$ for $1 \leqslant i \leqslant m$. We have

$$|N - \sigma q^{n-1}| \leqslant \left| N - \sum_{i=1}^{\sigma} N_i \right| + \sum_{i=1}^{\sigma} |N_i - q^{n-1}|.$$

For $\sigma + 1 \leqslant i \leqslant m$ we have that H_i is an $\mathbb{F}_q$-irreducible hypersurface which is not absolutely irreducible. Therefore, Lemma 2.3 implies

$$N - \sum_{i=1}^{\sigma} N_i \leqslant \sum_{i=\sigma+1}^{m} N_i < q^{n-2} \sum_{i=\sigma+1}^{m} \delta_i^2/4 \leqslant q^{n-2}\delta^2/4. \tag{24}$$

On the other hand, we have

$$\sum_{i=1}^{\sigma} N_i - N \leqslant \sum_{1 \leqslant i < j \leqslant \sigma} \#(H_i \cap H_j \cap \mathbb{F}_q^n) \leqslant q^{n-2} \sum_{1 \leqslant i < j \leqslant \sigma} \delta_i \delta_j \leqslant q^{n-2}\delta^2/2. \tag{25}$$

From (24) and (25) we conclude that the following estimate holds:

$$\left| N - \sum_{i=1}^{\sigma} N_i \right| \leqslant q^{n-2}\delta^2/2. \tag{26}$$

Since H_i is an absolutely irreducible $\mathbb{F}_q$-hypersurface of $\mathbb{A}^n$ for $1 \leqslant i \leqslant \sigma$, applying Theorem 5.2 we obtain

$$\begin{aligned} \sum_{i=1}^{\sigma} |N_i - q^{n-1}| &\leqslant q^{n-2} \sum_{i=1}^{\sigma} \left((\delta_i - 1)(\delta_i - 2)q^{1/2} + 5\delta_i^{\frac{13}{3}} \right) \\ &\leqslant \operatorname{sign}(\sigma)(\Delta - 1)(\Delta - 2)q^{n-\frac{3}{2}} + 5\Delta^{\frac{13}{3}} q^{n-2}. \end{aligned}$$

Combining this estimate with (26) finishes the proof of the theorem. □

6. From hypersurfaces to varieties

Let V be an equidimensional $\mathbb{F}_q$-variety of dimension $r > 0$ and degree δ. In this section we are going to exhibit a reduction of the problem of estimating the number of q-rational points of V to the hypersurface case. It is a well-known fact that a generic linear projection morphism $\pi : \mathbb{A}^n \to \mathbb{A}^{r+1}$ induces a birational morphism which maps V into a hypersurface of $\mathbb{A}^{r+1}$. Our next result yields an upper bound on the degree of the genericity condition underlying the choice of the projection morphism π.

Proposition 6.1. *Let $\Lambda := (\Lambda_{ij})_{1 \leqslant i \leqslant r+1, 1 \leqslant j \leqslant n}$ be an $(r+1) \times n$-matrix of indeterminates, let $\Lambda^{(i)} := (\Lambda_{i,1}, \ldots, \Lambda_{i,n})$ for $1 \leqslant i \leqslant r+1$, and let $\Gamma := (\Gamma_1, \ldots, \Gamma_{r+1})$ be an $(r+1)$-dimensional vector of indeterminates. Let $X := (X_1, \ldots, X_n)$ and let $\widetilde{Y} := \Lambda X + \Gamma$. Then there exists a nonzero polynomial $G \in \overline{\mathbb{F}}_q[\Lambda, \Gamma]$ of degree at most $2(r+1)\delta^2$ such that for any $(\lambda, \gamma) \in \mathbb{A}^{(r+1)n} \times \mathbb{A}^{r+1}$ with $G(\lambda, \gamma) \neq 0$ the following conditions are satisfied*:

(i) *Let $Y := \lambda X + \gamma := (Y_1, \ldots, Y_{r+1})$. Then the projection morphism $\pi : V \to \mathbb{A}^r$ defined by $Y_1, \ldots, Y_r$ is a finite morphism.*
(ii) *The linear form Y_{r+1} induces a primitive element of the integral ring extension $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$, i.e. the degree of its minimal integral dependence equation in $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$ equals the rank of $\overline{\mathbb{F}}_q[V]$ as (free) $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$-module.*

Proof. Let us consider the following morphism of algebraic varieties:

$$\begin{aligned} \Phi : \mathbb{A}^{(r+1)n} \times \mathbb{A}^{r+1} \times V &\to \mathbb{A}^{(r+1)n} \times \mathbb{A}^{r+1} \times \mathbb{A}^{r+1}, \\ (\lambda, \gamma, x) &\mapsto (\lambda, \gamma, \lambda x + \gamma). \end{aligned}$$

Using standard facts about Chow forms (see e.g. [Sha84,KPS01]), we conclude that $\overline{\mathrm{Im}(\Phi)}$ is a hypersurface of $\mathbb{A}^{(r+1)n} \times \mathbb{A}^{r+1} \times \mathbb{A}^{r+1}$, defined by a polynomial $P \in \overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{r+1}]$ which satisfies the following estimates:

- $\deg_{\widetilde{Y}_1,\ldots,\widetilde{Y}_{r+1}} P = \deg_{\widetilde{Y}_{r+1}} P = \delta$,
- $\deg_{\Lambda^{(i)},\,\Gamma_i} P \leqslant \delta$ for $1 \leqslant i \leqslant r+1$.

Let $G_1 \in \overline{\mathbb{F}}_q[\Lambda, \Gamma]$ be the (nonzero) coefficient of the monomial $\widetilde{Y}_{r+1}^{\delta}$ in the polynomial P, considering P as an element of $\overline{\mathbb{F}}_q[\Lambda, \Gamma][\widetilde{Y}_1, \ldots, \widetilde{Y}_{r+1}]$. We have $\deg G_1 \leqslant (r+1)\delta$. Let $\widetilde{G}_1 \in \overline{\mathbb{F}}_q[\Lambda^{(i)}, \Gamma_i : 1 \leqslant i \leqslant r]$ be the coefficient of a nonzero monomial of the polynomial G_1, considering G_1 as an element of $\overline{\mathbb{F}}_q[\Lambda^{(i)}, \Gamma_i : 1 \leqslant i \leqslant r][\Lambda^{(r+1)}, \Gamma_{r+1}]$.

Let $(\lambda^*, \gamma^*) \in \mathbb{A}^{rn} \times \mathbb{A}^r$ be any point satisfying the condition $\widetilde{G}_1(\lambda^*, \gamma^*) \neq 0$ and let $Y := (Y_1, \ldots, Y_r) := \lambda^* X + \gamma^*$. We claim that condition (i) of the statement of Proposition 6.1 holds. Indeed, since $G_1^* := G_1(\lambda^*, \gamma^*, \Lambda^{(r+1)}, \Gamma_{r+1})$ is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda^{(r+1)}, \Gamma_{r+1}]$, we deduce that there exist n $\overline{\mathbb{F}}_q$-linearly independent vectors $w_1, \ldots, w_n \in \overline{\mathbb{F}}_q^n$ and $a_1, \ldots, a_n \in \overline{\mathbb{F}}_q$ such that $G_1^*(w_k, a_k) \neq 0$ holds for $1 \leqslant k \leqslant n$. Let $\ell_k := w_k X + a_k$ for $1 \leqslant k \leqslant n$. By construction, for $1 \leqslant k \leqslant n$ the polynomial $P(\lambda^*, \gamma^*, w_k, a_k, Y_1, \ldots, Y_r, \ell_k)$ induces an integral dependence equation over $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$ for the coordinate function of $\overline{\mathbb{F}}_q[V]$ defined by ℓ_k. Since $\overline{\mathbb{F}}_q[\ell_1, \ldots, \ell_n] = \overline{\mathbb{F}}_q[X_1, \ldots, X_n]$ we conclude that condition (i) holds.

Furthermore, since $\overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_{r+1}]/(P)$ is a reduced $\overline{\mathbb{F}}_q$-algebra and $\overline{\mathbb{F}}_q$ is a perfect field, using [Mat80, Proposition 27.G] we see that the (zero-dimensional) $\overline{\mathbb{F}}_q(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r)$-algebra $\overline{\mathbb{F}}_q(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r)[\widetilde{Y}_{r+1}]/(P)$ is reduced. This implies that P is a separable element of $\overline{\mathbb{F}}_q(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r)[\widetilde{Y}_{r+1}]$, and hence P and $\partial P/\partial \widetilde{Y}_{r+1}$ are coprime in $\overline{\mathbb{F}}_q(\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r)[\widetilde{Y}_{r+1}]$. Then the discriminant $\rho := \mathrm{Res}_{\widetilde{Y}_{r+1}}(P, \partial P/\partial \widetilde{Y}_{r+1})$ of P with respect to $\widetilde{Y}_{r+1}$ is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda, \Gamma, \widetilde{Y}_1, \ldots, \widetilde{Y}_r]$ which satisfies the following degree estimates:

- $\deg_{\widetilde{Y}_1,\ldots,\widetilde{Y}_r} \rho \leqslant (2\delta - 1)\delta$,
- $\deg_{\Lambda^{(i)},\,\Gamma_i} \rho \leqslant (2\delta - 1)\delta$ for $1 \leqslant i \leqslant r+1$.

Let $\rho_1 \in \overline{\mathbb{F}}_q[\Lambda, \Gamma]$ be a (nonzero) coefficient of a monomial of ρ, considering ρ as an element of $\overline{\mathbb{F}}_q[\Lambda, \Gamma][\widetilde{Y}_1, \ldots, \widetilde{Y}_r]$ and let $G := \rho_1 \widetilde{G}_1$. Observe that $\deg G \leqslant 2(r+1)\delta^2$ holds.

Let $(\lambda, \gamma) \in \mathbb{A}^{(r+1)n} \times \mathbb{A}^{r+1}$ satisfy the condition $G(\lambda, \gamma) \neq 0$, let $(\lambda^*, \gamma^*) \in \mathbb{A}^{rn} \times \mathbb{A}^r$ be the first r rows of (λ, γ) and let $Y := (Y_1, \ldots, Y_{r+1}) = \lambda X + \gamma$. It is clear that condition (i) holds.

We are going to prove that condition (ii) holds. For this purpose, let ρ^* be the polynomial obtained from ρ by specializing $\Lambda^{(i)}, \Gamma_i$ $(1 \leqslant i \leqslant r)$ into the value (λ^*, γ^*). Then ρ^* is a nonzero polynomial of $\overline{\mathbb{F}}_q[\Lambda^{(r+1)}, \Gamma_{r+1}, Y_1, \ldots, Y_r]$ which equals the discriminant of $P(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, Y_1, \ldots, Y_r, \widetilde{Y}_{r+1})$ with respect to $\widetilde{Y}_{r+1}$.

Let $\xi_1, \ldots, \xi_n$ be the coordinate functions of V induced by $X_1, \ldots, X_n$, let $\zeta_i := \sum_{j=1}^n \lambda_{i,j}\xi_j$ for $1 \leqslant i \leqslant r$ and let $\widehat{Y}_{r+1} := \sum_{j=1}^n \Lambda_{r+1,j}\xi_j$. From the properties of the

Chow form of V we conclude that the identity

$$\begin{aligned} 0 &= P(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, \zeta_1, \ldots, \zeta_r, \widehat{Y}_{r+1}) \\ &= P(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, \zeta_1, \ldots, \zeta_r, \Lambda_{r+1,1}\xi_1 + \cdots + \Lambda_{r+1,n}\xi_n) \end{aligned} \tag{27}$$

holds in $\overline{\mathbb{F}}_q[\Lambda^{(r+1)}, \Gamma_{r+1}] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$. Following e.g. [ABRW96] or [Rou97], from (27) one deduces that for $1 \leqslant k \leqslant n$ the identity

$$\begin{aligned} &(\partial P/\partial \widetilde{Y}_{r+1})(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, \zeta_1, \ldots, \zeta_r, \widehat{Y}_{r+1})\xi_k \\ &\quad + (\partial P/\partial \Lambda_{r+1,k})(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, \zeta_1, \ldots, \zeta_r, \widehat{Y}_{r+1}) = 0 \end{aligned} \tag{28}$$

holds in $\overline{\mathbb{F}}_q[\Lambda^{(r+1)}, \Gamma_{r+1}] \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$. Since $\rho^*(\Lambda^{(r+1)}, \Gamma_{r+1}, Y_1, \ldots, Y_r)$ is the discriminant of $P(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, Y_1, \ldots, Y_r, \widetilde{Y}_{r+1})$ with respect to $\widetilde{Y}_{r+1}$, it can be expressed as a linear combination of $P(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, Y_1, \ldots, Y_r, \widetilde{Y}_{r+1})$ and $(\partial P/\partial \widetilde{Y}_{r+1})(\lambda^*, \Lambda^{(r+1)}, \gamma^*, \Gamma_{r+1}, Y_1, \ldots, Y_r, \widetilde{Y}_{r+1})$. Combining this observation with (27) and (28) we conclude that

$$\rho^*(\Lambda^{(r+1)}, \Gamma_{r+1}, \zeta_1, \ldots, \zeta_r)\xi_k + P_k(\Lambda^{(r+1)}, \Gamma_{r+1}, \zeta_1, \ldots, \zeta_r, \widehat{Y}_{r+1}) = 0 \tag{29}$$

holds, where P_k is a nonzero element of $\overline{\mathbb{F}}_q[\Lambda^{(r+1)}, \Gamma_{r+1}, Z_1, \ldots, Z_{r+1}]$ for $1 \leqslant i \leqslant n$. Specializing identity (29) into the values $\Lambda_{r+1,j} := \lambda_{r+1,j}$ $(1 \leqslant j \leqslant n)$ and $\Gamma_{r+1} = \gamma_{r+1}$ for $1 \leqslant k \leqslant n$ we conclude that Y_{r+1} induces a primitive element of the $\overline{\mathbb{F}}_q$-algebra extension $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r) \hookrightarrow \overline{\mathbb{F}}_q(Y_1, \ldots, Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$.

Condition (i) implies that $\overline{\mathbb{F}}_q[V]$ is a finite free $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$-module and hence $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$ is a finite-dimensional $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r)$-vector space. Furthermore, the dimension of $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$ as $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r)$-vector space equals the rank of $\overline{\mathbb{F}}_q[V]$ as $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$-module. On the other hand, since $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$ is integrally closed we have that the minimal dependence equation of any element of $f \in \overline{\mathbb{F}}_q[V]$ over $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r)$ equals the minimal integral dependence of f over $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r]$ (see e.g. [Kun85, Lemma II.2.15]). Combining this remark with the fact that Y_{r+1} induces a primitive element of the $\overline{\mathbb{F}}_q$-algebra extension $\overline{\mathbb{F}}_q(Y_1, \ldots, Y_r) \hookrightarrow \overline{\mathbb{F}}_q(Y_1, \ldots, Y_r) \otimes_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q[V]$ we conclude that Y_{r+1} also induces a primitive element of the $\overline{\mathbb{F}}_q$-algebra extension $\overline{\mathbb{F}}_q[Y_1, \ldots, Y_r] \hookrightarrow \overline{\mathbb{F}}_q[V]$. This shows condition (ii) and finishes the proof of the proposition. □

From Proposition 6.1 we easily deduce that V is birationally equivalent to an $\overline{\mathbb{F}}_q$-hypersurface $H \subset \mathbb{A}^{r+1}$ of degree δ, namely the image of V under the projection defined by linear forms $Y := (Y_1, \ldots, Y_{r+1}) = \lambda X + \gamma$ with $G(\lambda, \gamma) \neq 0$, where G is the polynomial of the statement of Proposition 6.1 (compare Proposition 6.3 below).

We would like to estimate the number of q-rational points of the variety V in terms of that of the hypersurface H, but "good" estimates on the number of q-rational points of H are not available if H is not an $\mathbb{F}_q$-variety. Let us observe that H is an $\mathbb{F}_q$-variety if the linear forms $Y_1, \ldots, Y_{r+1}$ belong to $\mathbb{F}_q[X_1, \ldots, X_n]$ (see e.g. [Kun85]). In order to ensure that there exist linear forms $Y_1, \ldots, Y_{r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ satisfying conditions (i) and (ii) of Proposition 6.1 we have the following result:

Corollary 6.2. *Let notations and assumptions be as in Proposition* 6.1. *If* $q > 2(r+1)\delta^2$, *there exists an element* $(\lambda, \gamma) \in \mathbb{F}_q^{(r+1)\times n} \times \mathbb{F}_q^{r+1}$ *satisfying the condition* $G(\lambda, \gamma) \neq 0$, *where* G *is the polynomial of the statement of Proposition* 6.1.

Proof. Let $V(G) := \{(\lambda, \gamma) \in \mathbb{A}^{(r+1)n} \times \mathbb{A}^{r+1} : G(\lambda, \gamma) = 0\}$. Taking into account the upper bound of Lemma 2.1

$$\#\big(V(G) \cap (\mathbb{F}_q^{(r+1)n} \times \mathbb{F}_q^{r+1})\big) \leqslant 2(r+1)\delta^2 q^{(r+1)(n+1)-1},$$

we immediately deduce the statement of Corollary 6.2. □

From now on, we shall assume that the condition $q > 2(r+1)\delta^2$ holds. Let $(\lambda, \gamma) \in \mathbb{F}_q^{(r+1)n} \times \mathbb{F}_q^{r+1}$ satisfy $G(\lambda, \gamma) \neq 0$, let $Y = (Y_1, \ldots, Y_{r+1}) := \lambda Y + \gamma$ and let us consider the following $\mathbb{F}_q$-definable morphism of $\mathbb{F}_q$-varieties:

$$\begin{aligned} \pi : V &\to \mathbb{A}^{r+1}, \\ x &\mapsto \big(Y_1(x), \ldots, Y_{r+1}(x)\big). \end{aligned}$$

Then the set $W := \pi(V)$ is an $\mathbb{F}_q$-hypersurface. This hypersurface is defined by a polynomial $h \in \mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$, which is a separable monic element of the polynomial ring $\mathbb{F}_q[Y_1, \ldots, Y_r][Y_{r+1}]$ of degree $\deg h = \deg_{Y_{r+1}} h = \delta$.

Let $V_1 \subset \mathbb{A}^n$ and $W_1 \subset \mathbb{A}^{r+1}$ be the following $\mathbb{F}_q$-varieties:

$$\begin{aligned} V_1 &:= \{x \in \mathbb{A}^n : (\partial h/\partial Y_{r+1})(Y_1(x), \ldots, Y_{r+1}(x)) = 0\}, \\ W_1 &:= \{y \in \mathbb{A}^{r+1} : (\partial h/\partial Y_{r+1})(y) = 0\}. \end{aligned}$$

Our following result shows that the variety V is birationally equivalent to the hypersurface $W \subset \mathbb{A}^{r+1}$.

Proposition 6.3. *Let* $q > 2(r+1)\delta^2$. *Then* $\pi|_{V\setminus V_1} : V\setminus V_1 \to W\setminus W_1$ *is an isomorphism of* $\mathbb{F}_q$*-Zariski open sets.*

Proof. Let us observe that $\pi(V\setminus V_1) \subset W\setminus W_1$. Then $\pi|_{V\setminus V_1} : V\setminus V_1 \to W\setminus W_1$ is a well-defined $\mathbb{F}_q$-definable morphism.

We claim that π is an injective mapping. Indeed, specializing identity (28) of the proof of Proposition 6.1 into the values $\Lambda_{r+1,j} := \lambda_{r+1,j}$ $(1 \leqslant j \leqslant n)$ and $\Gamma_{r+1} = \gamma_{r+1}$

we deduce that there exist polynomials $v_1, \ldots, v_n \in \mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$ such that for $1 \leqslant i \leqslant n$ the following identity holds:

$$v_i(Y_1, \ldots, Y_{r+1}) - X_i \cdot (\partial h/\partial Y_{r+1})(Y_1, \ldots, Y_{r+1}) \equiv 0 \bmod I(V). \tag{30}$$

Let $x := (x_1, \ldots, x_n), x' := (x'_1, \ldots, x'_n) \in V \backslash V_1$ satisfy $\pi(x) = \pi(x')$. We have $Y_i(x) = Y_i(x')$ for $1 \leqslant i \leqslant r+1$. Then from (30) we conclude that $x_i = x'_i$ for $1 \leqslant i \leqslant n$, which shows our claim.

Now we show that $\pi|_{V\backslash V_1} : V \backslash V_1 \to W \backslash W_1$ is a surjective mapping. Let $h_0 := \partial h/\partial Y_{r+1}$. Let be given an arbitrary element $y := (y_1, \ldots, y_{r+1})$ of $W \backslash W_1$, and let

$$x := \big((v_1/h_0)(y), \ldots, (v_n/h_0)(y)\big).$$

We claim that x belongs to $V \backslash V_1$. Indeed, let f be an arbitrary element of the ideal $I(V)$ and let $\tilde{f} := (h_0(Y_1, \ldots, Y_{r+1}))^N f$, where $N := \deg f$. Then there exists $g \in \mathbb{F}_q[Z_1, \ldots, Z_{n+1}]$ such that $\tilde{f} = g(h_0 X_1, \ldots, h_0 X_n, h_0)$ holds. Since $\tilde{f} \in I(V)$, for any $z \in V$ we have $\tilde{f}(z) = 0$ and hence from identity (30) we conclude that $g(v_1, \ldots, v_n, h_0)\big(Y_1(z), \ldots, Y_{r+1}(z)\big) = 0$ holds. This shows that h divides $\hat{f} := g(v_1, \ldots, v_n, h_0)$ in $\mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$ and therefore $\hat{f}(y) = h_0(y)^N f(x) = 0$ holds. Taking into account that $h_0(y) \neq 0$ we conclude that $f(x) = 0$ holds, i.e. $x \in V \backslash V_1$.

In order to finish the proof of the surjectivity of π there remains to prove that $\pi(x) = y$ holds. For this purpose, we observe that identity (30) shows that any $z \in V$ satisfies

$$Y_i(z) h_0\big(Y_1(z), \ldots, Y_{r+1}(z)\big) - \sum_{j=1}^{n} \lambda_{i,j}\, v_j\big(Y_1(z), \ldots, Y_{r+1}(z)\big) = 0$$

for $1 \leqslant i \leqslant r+1$. Then h divides the polynomial $Y_i h_0 - \sum_{j=1}^n \lambda_{i,j} v_j$ in $\mathbb{F}_q[Y_1, \ldots Y_{r+1}]$, which implies $y_i = \sum_{j=1}^n \lambda_{i,j}(v_j/h_0)(y) = \sum_{j=1}^n \lambda_{i,j}\, x_j$ for $1 \leqslant i \leqslant r+1$. This proves that $\pi(x) = y$ holds.

Finally we show that $\pi|_{V\backslash V_1} : V \backslash V_1 \to W \backslash W_1$ is an isomorphism. Let

$$\begin{aligned} \phi : W \backslash W_1 &\to V \backslash V_1, \\ y &\mapsto \big((v_1/h_0)(y), \ldots, (v_n/h_0)(y)\big). \end{aligned}$$

Our previous discussion shows that ϕ is a well-defined $\mathbb{F}_q$-definable morphism and $\pi \circ \phi$ is the identity mapping of $W \backslash W_1$. This finishes the proof of the proposition. □

From Proposition 6.3 we immediately conclude that the $\mathbb{F}_q$-Zariski open sets $V \backslash V_1$ and $W \backslash W_1$ have the same number of q-rational points.

7. Estimates for an $\mathbb{F}_q$-variety

In this section we exhibit explicit estimates on the number of q-rational points of an $\mathbb{F}_q$-variety. For this purpose, we are going to apply the reduction to the hypersurface case of Section 6, together with the estimates for hypersurfaces of Section 5. We start with the case of an absolutely irreducible $\mathbb{F}_q$-variety.

Theorem 7.1. *Let $V \subset \mathbb{A}^n$ be an absolutely irreducible $\mathbb{F}_q$-variety of dimension $r > 0$ and degree δ. If $q > 2(r+1)\delta^2$, then the following estimate holds*:

$$|\#(V \cap \mathbb{F}_q{}^n) - q^r| \leqslant (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + 5\delta^{\frac{13}{3}}q^{r-1}. \tag{31}$$

Proof. First we observe that the theorem is obviously true in the cases $n = 1$ or $\delta = 1$, and follows from Weil's estimate (1) in the case $n = 2$. Therefore, we may assume without loss of generality that $n \geqslant 3$ and $\delta \geqslant 2$ hold.

Since the condition $q > 2(r+1)\delta^2$ holds, from Corollary 6.2 we deduce that there exist linear forms $Y_1, \ldots, Y_{r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ satisfying conditions (i) and (ii) of the statement of Proposition 6.1. Therefore, from Proposition 6.3 we have

$$|\#(V \cap \mathbb{F}_q^n) - q^r| \leqslant |\#(W \cap \mathbb{F}_q^{r+1}) - q^r| + \#(V \cap V_1 \cap \mathbb{F}_q^n) + \#(W \cap W_1 \cap \mathbb{F}_q^{r+1}),$$

where $V_1 \subset \mathbb{A}^n$, $W \subset \mathbb{A}^{r+1}$ and $W_1 \subset \mathbb{A}^{r+1}$ are the $\mathbb{F}_q$-hypersurfaces defined by the polynomials $(\partial h/\partial Y_{r+1})\big(Y_1(X), \ldots, Y_{r+1}(X)\big) \in \mathbb{F}_q[X_1, \ldots, X_n]$, $h \in \mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$ and $(\partial h/\partial Y_{r+1}) \in \mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$, respectively.

From the Bézout inequality (7) and Lemma 2.1 we deduce the upper bounds:

$$\begin{aligned} \#(V \cap V_1 \cap \mathbb{F}_q^n) &\leqslant \delta(\delta-1)q^{r-1}, \\ \#(W \cap W_1 \cap \mathbb{F}_q^{r+1}) &\leqslant \delta(\delta-1)q^{r-1}. \end{aligned} \tag{32}$$

On the other hand, we observe that W is an absolutely irreducible $\mathbb{F}_q$-variety of dimension $r > 0$ and degree $\delta > 0$. Therefore, applying the estimate in the third line of (22) we obtain

$$|\#(W \cap \mathbb{F}_q^{r+1}) - q^r| \leqslant (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + \left(\tfrac{8}{3}\delta^{\frac{13}{3}} + 4\delta^{\frac{11}{3}} + 2\delta^2 + \delta + \tfrac{7}{3}\right)q^{r-1}.$$

This estimate, together with (32), immediately implies the statement of the theorem for $\delta \geqslant 3$. For $\delta = 2$ we combine the above estimate with (32) and the second line of (23), which yields the estimate of the statement of the theorem. This finishes the proof. □

Furthermore, if we estimate $|\#(W \cap \mathbb{F}_q^{r+1}) - q^r|$ using Theorem 5.3 instead of Theorem 5.2, we obtain the following result:

Corollary 7.2. *Let $V \subset \mathbb{A}^n$ be an absolutely irreducible $\mathbb{F}_q$-variety of dimension $r > 0$ and degree δ. If $q > \max\{2(r+1)\delta^2, 15\delta^{\frac{13}{3}}\}$, then the following estimate holds*:

$$|\#(V \cap \mathbb{F}_q^{r+1}) - q^r| \leqslant (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + 7\delta^2 q^{r-1}.$$

Finally, if the characteristic p of $\mathbb{F}_q$ is greater than $2\delta^2$, from Corollary 5.6 we obtain:

Corollary 7.3. *Let $V \subset \mathbb{A}^n$ be an absolutely irreducible $\mathbb{F}_q$-variety of dimension $r > 0$ and degree δ. If $p > 2\delta^2$ and $q > 2(r+1)\delta^2$ we have*

$$|\#(V \cap \mathbb{F}_q^{r+1}) - q^r| \leqslant (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + 4\delta^4 q^{r-1}.$$

If in addition $q > 27\delta^4$, then the following estimate holds:

$$|\#(V \cap \mathbb{F}_q^{r+1}) - q^r| \leqslant (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + 7\delta^2 q^{r-1}.$$

The estimate of Theorem 7.1 yields a nontrivial lower bound on the number of q-rational points of an absolutely irreducible $\mathbb{F}_q$-variety V of dimension $r > 0$ and degree δ, implying thus the existence of a q-rational point of V, for $q > \max\{2(r+1)\delta^2, 9\delta^{\frac{13}{3}}\}$. Nevertheless, similarly to Theorem 5.4, the following simple argument allows us to obtain the following improved existence result:

Corollary 7.4. *For $q > \max\{2(r+1)\delta^2, 2\delta^4\}$, any absolutely irreducible $\mathbb{F}_q$-variety V of dimension $r > 0$ and degree δ has a q-rational point.*

Proof. Since $q > 2(r+1)\delta^2$ holds, from Corollary 6.2 we conclude that there exist linear forms $Y_1, \ldots, Y_{r+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ satisfying the conditions of Proposition 6.1. Let $h \in \mathbb{F}_q[Y_1, \ldots, Y_{r+1}]$ denote the defining polynomial of the absolutely irreducible $\mathbb{F}_q$-hypersurface $W \subset \mathbb{A}^{r+1}$ defined by the image of the linear projection of V induced by $Y_1, \ldots, Y_{r+1}$. From the condition $q > 2\delta^4$ we conclude that there exists an $\mathbb{F}_q$-plane $L \subset \mathbb{A}^{r+1}$ for which $W \cap L$ is an absolutely irreducible $\mathbb{F}_q$-curve of $\mathbb{A}^{r+1}$. Hence, Weil's estimate (1) shows that $\#(W \cap L \cap \mathbb{F}_q^{r+1}) \geqslant q - (\delta-1)(\delta-2)q^{\frac{1}{2}} - \delta - 1$ holds. Furthermore, from the Bézout inequality we deduce that $\#(W \cap L \cap V(\partial h/\partial Y_{r+1})) \leqslant \delta(\delta-1)$ holds, which implies $\#\left(\left(W \setminus V(\partial h/\partial Y_{r+1})\right) \cap L \cap \mathbb{F}_q^{r+1}\right) \geqslant q - (\delta-1)(\delta-2)q^{\frac{1}{2}} - \delta^2 - 1$. Since this quantity is strictly positive for $q > 2\delta^4$, it follows that there exists a q-rational point of $W \setminus V(\partial h/\partial Y_{r+1})$. Combining this with Proposition 6.3 we conclude that there exists a q-rational point of V. □

7.1. An estimate for an arbitrary $\mathbb{F}_q$-variety

Now we are going to estimate the number of q-rational points of an arbitrary $\mathbb{F}_q$-variety V of dimension $r > 0$ and degree δ. Let $V = V_1 \cup \cdots \cup V_m$ be the decomposition of V into $\mathbb{F}_q$-irreducible components and suppose that the numbering is such that V_i is absolutely irreducible of dimension $r > 0$ for $1 \leqslant i \leqslant \sigma$, absolutely irreducible of dimension at most $r-1$ for $\sigma+1 \leqslant i \leqslant \rho$ and not absolutely irreducible for $\rho+1 \leqslant i \leqslant m$.

For $1 \leqslant i \leqslant m$, let $N_i := \#(V_i \cap \mathbb{F}_q^n)$ and denote by δ_i the degree of V_i. Finally, let $\Delta := \sum_{i=1}^{\sigma} \delta_i$ and $N := \#(V \cap \mathbb{F}_q^n)$. We have the following result:

Theorem 7.5. *With notations and assumptions as above, if $q > 2(r+1)\delta^2$ the number N of q-rational points of the variety V satisfies the following estimate*:

$$|N - \sigma q^r| \leqslant \operatorname{sign}(\sigma)(\Delta - 1)(\Delta - 2)q^{r-1/2} + \left(5\Delta^{\frac{13}{3}} + \delta^2\right)q^{r-1}, \tag{33}$$

where $\operatorname{sign}(\sigma) := 0$ *for* $\sigma = 0$ *and* $\operatorname{sign}(\sigma) := 1$ *otherwise*.

Proof. We have $|N - \sigma q^r| \leqslant \sum_{i=1}^{\sigma} |N_i - q^r| + |N - \sum_{i=1}^{\sigma} N_i|$.

From Theorem 7.1 we obtain

$$\begin{aligned} \sum_{i=1}^{\sigma} |N_i - q^r| &\leqslant \sum_{i=1}^{\sigma} \left((\delta_i - 1)(\delta_i - 2)q^{r-1/2} + 5\delta_i^{\frac{13}{3}} q^{r-1}\right) \\ &\leqslant \operatorname{sign}(\sigma)(\Delta - 1)(\Delta - 2)q^{r-1/2} + 5\Delta^{\frac{13}{3}} q^{r-1}. \end{aligned} \tag{34}$$

Now we estimate the term $|N - \sum_{i=1}^{\sigma} N_i|$. Let $\sigma + 1 \leqslant i \leqslant \rho$. Then V_i is an $\mathbb{F}_q$-variety of dimension at most $r-1$ and degree δ_i, and Lemma 2.1 implies $N_i \leqslant \delta_i q^{r-1}$. On the other hand, for $\rho + 1 \leqslant i \leqslant m$ we have that V_i is $\mathbb{F}_q$-irreducible and not absolutely irreducible, and Lemma 2.3 shows that $N_i \leqslant \delta_i^2 q^{r-1}/4$ holds. Then we have

$$N - \sum_{i=1}^{\sigma} N_i \leqslant \sum_{i=\sigma+1}^{m} N_i \leqslant q^{r-1} \sum_{i=\sigma+1}^{m} \delta_i^2 \leqslant \delta^2 q^{r-1}. \tag{35}$$

On the other hand, Lemma 2.1 implies

$$\sum_{i=1}^{\sigma} N_i - N \leqslant \sum_{1 \leqslant i < j \leqslant \sigma} \#(V_i \cap V_j \cap \mathbb{F}_q^n) \leqslant q^{r-1} \sum_{1 \leqslant i < j \leqslant \sigma} \delta_i \delta_j \leqslant \delta^2 q^{r-1}/2. \tag{36}$$

From estimates (35) and (36) we conclude that $|N - \sum_{i=1}^{\sigma} N_i| \leqslant \delta^2 q^{r-1}$ holds. Combining this estimate with (34) finishes the proof of the theorem. □

Acknowledgments

The authors are indebted to Joos Heintz for having strongly inspired this work. A. Cafure also thanks Robert Rolland for his helpful remarks.

References

[ABRW96] M.E. Alonso, E. Becker, M.-F. Roy, T. Wörmann, Zeroes, multiplicities and idempotents for zerodimensional systems, in: Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94, Progress in Mathematics, vol. 143, Birkhäuser, Boston, 1996, pp. 1–15.

[Bom74] E. Bombieri, Counting points on curves over finite fields (d'après S.A. Stepanov), Exp 430, in: Séminaire Bourbaki 1972/1973, Lecture Notes in Mathematics, vol. 383, Springer, New York, 1974, pp. 234–241.

[CM02] A. Cafure, G. Matera, Explicit estimates for the number of solutions of polynomial equation systems over finite fields, in: P. D'Argenio, G. Matera (Eds.), Proceedings Workshop Argentino de Informática Teórica, WAIT'02, Santa Fe, Argentina, September 2002, Anales Jornadas Argentinas de Informática e Investigación Operativa, vol. 31, SADIO, 2002, Buenos Aires, pp. 26–41.

[CM03] A. Cafure, G. Matera, Fast computation of a rational point of a variety over a finite field, Manuscript Universidad Nacional de General. Sarmiento, 2003. Available at http://arxiv.org/abs/math.NT/0406085.

[CR96] J.P. Cherdieu, R. Rolland, On the number of points of some hypersurfaces in $\mathbb{F}_q^n$, Finite Fields Appl. 2 (2) (1996) 214–224.

[Ful84] W. Fulton, Intersection Theory, Springer, Berlin, Heidelberg, New York, 1984.

[Gao03] S. Gao, Factoring multivariate polynomials via partial differential equations, Math. Comp. 72 (2003) 801–822.

[GL02a] S. Ghorpade, G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, Moscow Math. J. 2 (3) (2002) 589–631.

[GL02b] S. Ghorpade, G. Lachaud, Number of solutions of equations over finite fields and a conjecture of Lang and Weil, in: A.K. Agarwal et al. (Eds.), Number Theory and Discrete Mathematics (Chandigarh, 2000), Hindustan Book Agency, New Delhi, 2002, pp. 269–291.

[Hei83] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.

[HS82] J. Heintz, C.P. Schnorr, Testing polynomials which are easy to compute, in: International Symposium on Logic and Algorithmic, Zurich 1980, Monographies de L'Enseignement Mathematiques, vol. 30, 1982, pp. 237–254.

[HW98] M.-D. Huang, Y.-C. Wong, An algorithm for approximate counting of points on algebraic sets over finite fields, in: J. Buhler (Ed.), Third International Symposium on Algorithmic Number Theory, ANTS-III, Portland, Oregon, USA, June 21–25, 1998, Lecture Notes in Computer Science, vol. 1423, Springer, Berlin, 1998, pp. 514–527.

[HW99] M.-D. Huang, Y.-C. Wong, Solvability of systems of polynomial congruences modulo a large prime, Comput. Complexity 8 (1999) 227–257.

[Kal95] E. Kaltofen, Effective Noether irreducibility forms and applications, J. Comput. System Sci. 50 (2) (1995) 274–295.

[KPS01] T. Krick, L.M. Pardo, M. Sombra, Sharp estimates for the Arithmetic Nullstellensatz, Duke Math. J. 109 (3) (2001) 521–598.

[Kun85] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, 1985.

[LN83] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, MA, 1983.

[LW54] S. Lang, A. Weil, The number of points of varieties in finite fields, Amer. J. Math. 76 (1954) 819–827.

[Mat80] H. Matsumura, Commutative Algebra, Benjamin, New York, 1980.

[Rou97] F. Rouillier, Solving zero-dimensional systems through rational univariate representation, Appl. Algebra Eng. Comm. Comput. 9 (5) (1997) 433–461.

[Sch73] W. Schmidt, Zur Methode von Stepanov, Acta Arith. 24 (1973) 347–367.

[Sch74] W. Schmidt, A lower bound for the number of solutions of equations over finite fields, J. Number Theory 6 (6) (1974) 448–480.

[Sch76] W. Schmidt, Equations over Finite Fields: An Elementary Approach, Lectures Notes in Mathematics, vol. 536, Springer, New York, 1976.

[Sha84] I.R. Shafarevich, Basic Algebraic Geometry, Graduate Texts in Mathematics, Springer, New York, 1984.

[Sha94] I.R. Shafarevich, Basic Algebraic Geometry: Varieties in Projective Space, Springer, Berlin, Heidelberg, New York, 1994.

[Ste71] S. Stepanov, On the number of points of a hyperelliptic curve over a finite prime field, Math. USSR Izv. 3 (1971) 1103–1114.

[Wei48] A. Weil, Sur les Courbes Algébriques et les Varietés Qui s'en Déduisent, Hermann, Paris, 1948.